When the world went virtual overnight

5 smart products we could do with right now

₹125

VOL. 33 | ISSUE 5 | MAY 2020

PCQUEST

www.pcquest.com

UNDERSTAND • CHOOSE • IMPLEMENT IT

Indian drone startups turn themselves into Force Multipliers during lockdown

Corona Criminals Strike

Hackers take advantage of pandemic: Here's what you can do

Special Subscription offer on page 62

76 pages including cover

New Leader.
New Rules.

Raise expectations
for your data center.

AMD
EPYC

CyberMedia

PCQUEST

Never Miss Out An Opportunity To Reach A Wider Audience With

WEBINARS

on

SECURITY | **DATA STORAGE/ CLOUD** | **COLLABORATION** | **BUSINESS CONTINUITY PLANNING**

and many more...

- Communicate with hundreds of people from anywhere in the world
- Keep your audience Engaged
- Generate new Leads
- Qualify new leads and build Relationships
- Speed up sales process and get ROI faster

WHO TO ATTEND

- IT Decision Makers
- IT Managers
- IT Influencers
- Network Heads
- Network Managers
- IT Security Professionals
- Business Users
- And more...

***Verticals*: BFSI, Manufacturing, IT/ITeS/Logistics/Healthcare, e-commerce**

Contact Us: Marketing & Alliance

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

Contents

MAY 2020

SUBSCRIBE NOW!

Turn to page 62

PCQUEST
UNDERSTAND • CHOOSE • IMPLEMENT IT

CyberMedia

For subscription queries contact: rsepcq@cybermedia.co.in
Send all your tech questions to: pcquest@cybermedia.co.in

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 Karan Printers, F 29/2, Phase II, Okhla Industrial Area, 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.

www.pcquest.com | http://twitter.com/pcquest | http://facebook.com/pcquest | http://linkd.in/pcquest | http://gplus.to/pcquest | pcquest@cybermedia.co.in

Sunil Rajguru, Editor
sunilr@cybermedia.co.in

Time to upgrade the world

The times they are a changing… no… the times have changed! The sooner we realize this, the easier it will be for us to move on and plan a new world. We hope that the Covid-19 crisis is firmly put behind us, but future pandemic alerts could be the norm. That is why we have to upgrade the world accordingly and put technology to good use.

Do you really need to travel to that far off place when a series of video calls would do? The collaboration industry has finally come of age with the likes of Zoom, file sharing and even 3D tools. When things return back to normal we can decide to commute, do domestic and foreign travel only sparingly. Videoconferencing has to be the first choice and only if that doesn't work should travel be decided upon.

> ***We need a change in legislation***

How many Work From Home jobs don't materialize because the company is too suspicious or the boss wants to have a team in a physical location to lord over? It's time to kick the ego and take a proper WFH policy. If any job can be WFHed and the right candidate can be found then one should go ahead with it.

If 5G is not coming nationwide, then it should just be implemented in city centres and the rest of the country should be connected via laying even more optic fibre cables, having mobile Wi-Fi hotspots (via drones, weather balloons or even blimps) and maybe even expand and boost a 4G network in an area which may leapfrog to 6G someday.

Education is ripe for reform. School can be boosted with online tools but those in far off places can benefit from virtual classrooms. While school children studying at home on the laptop with working parents may be impractical; not so with college. An adult student who does multiple relevant online courses at home to develop the right skills may be preferred over one who goes to an expensive college to get an outdated degree.

Legislation is the only thing holding back drones and driverless cars. The government should push them with strict safety measures. It can be done in a phased manner so laws can be amended regularly to ensure safety. That's the same with physical robots. The government should also accelerate the digitization process of its archaic departments and boost national data centres. Sport stars should consider participating in virtual tournaments.

Finally the future belongs to Big Data, Artificial Intelligence, Machine Learning and Natural Language Processing. We need many more courses, professionals and projects for the same. Welcome to yet another upgrade!

Sunil Rajguru

A SPUR OF CYBER ATTACKS DURING THE PANDEMIC

Cybercriminals are quick in spotting a chance to make a profit, especially when the majority of users are concerned with an ongoing global pandemic

Ashok Pandey
ashokpa@cybermedia.co.in

Cyberthreats are constantly evolving, cybercriminals are targeting computer and other devices in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. IT has caused the global disruption, also has changed the cybersecurity threat landscape.

There has been an increase in the number of cybercrimes since professionals were asked to work from home. The national cybersecurity agency CERT-In stated that "Cybercriminals are exploiting the COVID-19 outbreak as an opportunity".

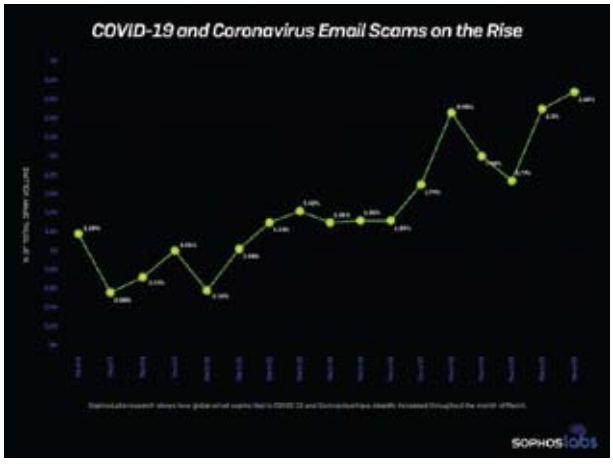
Attacks broadly fall under 4 categories - Phishing, injecting malware/ransomware, peddling things of dubious utility and malicious targeting of people/communities.

WHO reports fivefold increase in cyber attacks, last week they reported some that 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response. The number of cyberattacks is now more than five times the number directed at the Organization in the same period last year.

"Ensuring the security of health information for Member States and the privacy of users interacting with us a priority for WHO at all times, but also particularly during the COVID-19 pandemic. We are grateful for the alerts we receive from Member States and the private sector. We are all in this fight together," said Bernardo Mariano, WHO's Chief Information Officer.

The surge of spam

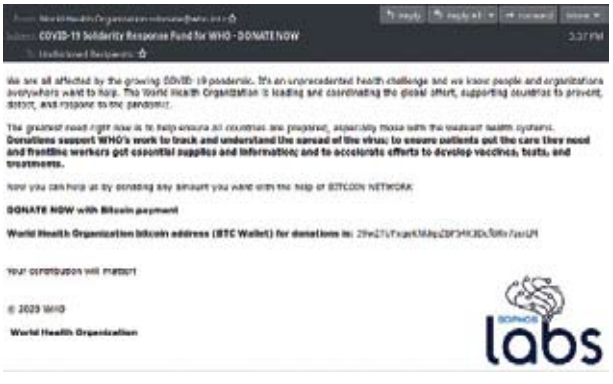
Sophos measured a significant percentage of the



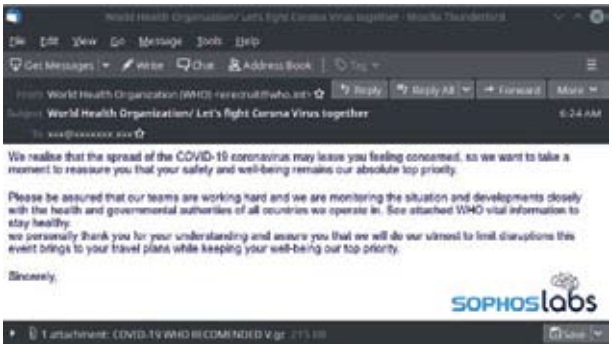
spam traffic by early March.

Spam campaigns detected by Sophos

- A sextortion scheme threatening to infect the target's family with COVID-19 if they didn't pay.
- A scam purporting to be a fundraising



plea from the World Health Organization, asking for donations in Bitcoin to fund COVID-19 research.



- Messages purportedly from WHO, but carrying documents with dropper malware.
- Marketing for "emergency supplies," including filter masks.
- A sales pitch for a $37 video download,

purporting to offer insider information from a "military source" on how to survive Coronavirus

- COVID-19 related extortion scams detected and blocked by Sophos

Hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic and sending fraudulent email and

"We are seeing a spike in the number of ransomware, phishing attacks through malicious links and apps to hack devices and steal data. We are also witnessing 'Back to school' ransomware attacks which are heavily targeting K-12 and academic institutions for higher learning. As the global workforce shifts to work-from-home deployments, organizations are operationalizing a much larger group of remote users, making virtual private networks (VPNs) more critical than ever before. In fact, SonicWall has seen a 1,766% increase in VPN-SSL customers quarter-to-date."

—Debasish Mukherjee, VP, Regional Sales APAC, SonicWall

"Cybercriminals have taken advantage of the health crisis to target users in a variety of ways, including leveraging it in malicious emails to phish users and spread digital viruses. The tactic of using current affairs to make scams more relevant isn't new. We've seen similar types of scams associated with natural disasters and popular global events in the past. This pandemic has once again provided cybercriminals with another route to peddle their malware and steal login credentials by playing on people's fears. As more employees in India work from home, they need to be mindful that clicking on phishing emails from their personal devices can introduce new threats and put the wider corporate network at risk."

—Diwakar Dayal, MD, Tenable, India

Quick Facts

- During Q1 2020, the Gulf Cooperation Council (GCC) recorded 1,737 email spam attacks
- Worldwide, Trend Micro blocked more than 907,000 spam messages
- Google detected over 18 million daily malware and phishing emails
- Trend Micro recorded more than 48,000 hits on malicious URLs and detected 737 malware threats
- URL attacks increased 260x and email spam attacks increased 220x from February 2020-March 2020.

WhatsApp messages to trick people into clicking on malicious links or opening attachments. Once the user clicks on the link, it can reveal their user name and password, which can be used to steal money or sensitive information.

In a blog post, Google stated that the company detected over 18 million daily malware and phishing emails related to Covid-19 on its platform. "Every day, Gmail blocks more than 100 million phishing emails. During the last week, we saw 18 million daily malware and phishing emails related to Covid-19. This is in addition to more than 240 million COVID-related daily spam messages," the post read.

Spam campaigns detected by Symantec

Symantec came across dozens of new malicious email campaigns. The scammers have employed a range of tactics in a bid to evade detection, including various email templates, "From" addresses, IP addresses, and URL domains.

Symantec analysed the email campaigns, while earlier it was dominated by phishing and MalSpam (malware bearing) emails. Later on, snowshoe spam took over as the most common form of campaign, accounting for more than 40 per cent of all emails blocked by Symantec. This was following by phishing (30 per cent), MalSpam (18 per cent), and scams (9 per cent).

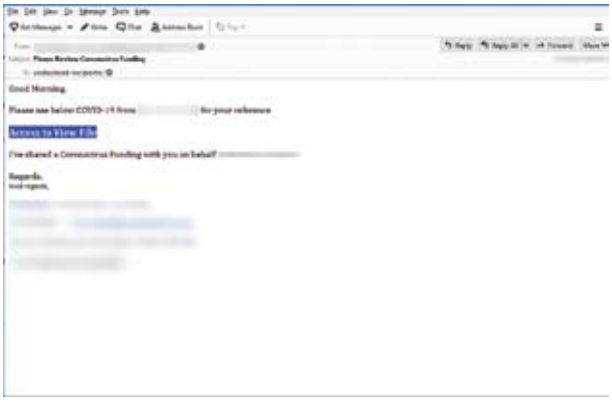
There was a sharp uptick in the number of malicious emails blocked by Symantec on March 16, with a surge of spam runs focused around selling face masks, medical equipment, immunity oil, and other products related to COVID-19 virus outbreak.

• **CDC phishing emails:** Phishing email purporting to come from the U.S. Centers for Disease Control and Prevention (CDC)

The email was crafted to appear as a message from the U.S. Centers for Disease Control and Prevention (CDC). So the recipient shall click on the

link, the link text appears to be "cdcinfo.gov", but it takes the user to a malicious URL.

• **Phishing email disguised as funding proposal:** The phishing campaign used a short template to



masquerade as a legitimate business email.

The email urges to review coronavirus funding proposals, with "Access to View File" hyperlinking to

"The current pandemic situation has created a perfect storm for Cybercriminals to capitalize on the latest trends to try and boost the success rates of attacks. The malware and cybersecurity attacks have been hitting all over and due to increased hacker activity; phishing attempts have gone up by three times It has been noticed that the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 1,200 complaints related to COVID-19 scams and one of the major threats observed in India was AZORult — a malware designed to steal information including credentials and take data from your computer including passwords and cryptographic forms of money. This malware first discovered in 2016 but was recently linked with malicious files and apps belonging to the COVID-19 theme."

—Prashanth G J, CEO, TechnoBind

"Most companies are working remotely today, which has increased the susceptibility of cyber attacks and the theft of sensitive data. The hackers are sending unsafe links of people that can lead to the theft of sensitive data. At the current scenario, the role of cybersecurity has become more sensitive matter, the layer of security on home Wi-Fi systems are low. Cybercriminals are taking more advantage of capitalism and access data which otherwise is secure. Nowadays, small business & medical sector are most vulnerable to cyber-attacks. Therefore, there is a need to make the cybersecurity industry more dynamic and responsive than ever before. Yes, we have seen that Cyber Criminals are adopting different types of Tactics, due to which digital fraud is increasing rapidly. Similar to what Lt Gen. Pant of NCSC said, there has been a huge number of fraud portals related to Corona Virus have been created across the globe by cybercriminals. Additionally, people are receiving fake infected maps, that also requires the users to download the software, follow the steps, which is a concern for data security of people. Also, individuals are receiving unknown calls from fraud call centres; asking them to share their personal bank details to increase their limits, on the other side, many people are getting fake messages and links as well."

—Trishneet Arora, Founder & CEO, TAC Security

"When critical situations arise that prey on human concerns, there are often added cyber risks in the form of bad actors trying to capitalise on people's fears. The current global health crisis is no different, with the WHO warning of hackers launching carefully coordinated phishing emails purporting to offer updates on the situation. In the Czech Republic, reports also indicate that hackers are targeting hospitals fighting the outbreak with ransomware attacks, showing the lengths hackers will go to in pursuit of monetary gain."

—Rohan Vaidya, Regional Director of Sales - India, CyberArk

"Opportunism is the hallmark of cybercriminals. They constantly hone their tactics of orchestrating cyber-attacks. Whether it is cyber criminals, scammers, or opportunists, the current situation has proven to be the perfect time for them to target users in a variety of ways. These include phishing, business email compromise (BEC), malware, ransomware, fake websites, domain squatting, and spam. Unsurprisingly, when it comes to malicious activity, we have seen a rise in unwanted emails (malicious, spam, or phishing) containing embedded URLs using the keywords of COVID or Coronavirus. Malicious coronavirus-themed emails try to instill a sense of urgency in end users, encouraging them to undertake tasks such as submit personal data or reset company passwords. Even, many new websites – both malicious and legitimate – were registered in March and early April with COVID or Coronavirus-themed domains. There were many spikes in browsing activity, one of which can be explained by an interest in a legitimate Indian Covid-19 tracking site that correlated with an order prescribing lockdown in the country. Whether employees are using work-issued laptops or accessing files from their home computers, we must be vigilant and double-check any requests which seemingly come from official sources."

—Surendra Singh, Senior Director & Country Manager, Forcepoint

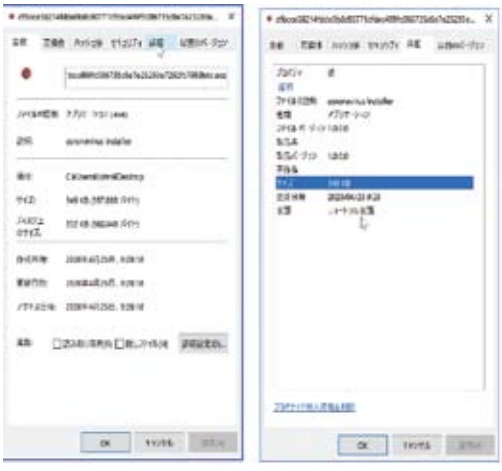
an online document. When the viewer clicks on the link, it asks for their credentials.

- **Advance fee fraud scam:** One example of a COVID-19 themed scam campaign seen by Symantec is an email pretending to come from the World Health

Organization (WHO) and appears to be a classic example of advance fee fraud.

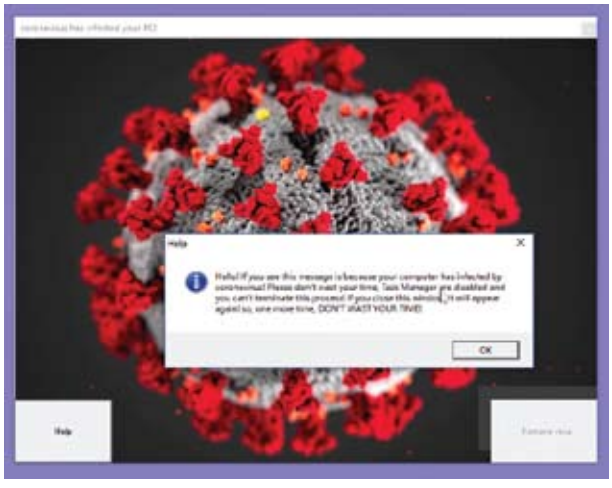
- **COVID-19 themed extortion attempt:** In this scam campaign, the sender claims to be a neighbour of the recipient who has been diagnosed with COVID-19. He tried to threaten to infect the recipient's home unless they pay them.
- **Surgical mask spam:** Another spam campaign claimed to come from a surgical mask supplier in China and now asking the receiver to purchase from them and then sell.

Recently, Trend Micro Research analyzed coronavirus-themed malware. This malware overrides systems' master boot record (MBR), making it unbootable and has "Coronavirus



"Cybercriminals have been exploiting fears of the people around the COVID-19 outbreak to find ways to hack their digital space and the most common and widely seen crime is by conducting email scams, phishing and ransomware attacks. These emails and messages entice users to open malicious attachments by offering more information related to the COVID-19 situation but contain malicious files masked under the guise of links, pdf, mp4 or Docx files."

—Anil Bhasin, regional vice president, India & SAARC, Palo Alto Networks



Installer" in the description.

When the malware executed, the infected PC will restart automatically and then displays a virus-themed window that cannot be closed. Clicking on any button won't work including, Help and Remove virus.

Trend Micro Research also analyzed a Covid-19 themed malicious HTA file based on the command and control infrastructure. This HTA file contained a pop-up PDF lure displaying clickbait titles and images of the Pakistan army. It was connected with below mentioned malicious URLs:

- hxxp[://www.d01fa[.net/plugins/16364/11542/true/true/
- hxxp[://www.d01fa[.net/cgi/8ee4d36866/16364/11542/58a3a04b/file.hta
- hxxps[://cloud-apt[.net/202/6eX0Z6GW9pNVk25yO0x7DqKJzaNm6LIRaR0GCukX/16364/11542/2a441439

"From what we can see, fake shops are the most common type of scam, selling discounted medical equipment, like face masks or hand sanitizer. Some are even claiming to sell treatments or at home COVID-19 tests. Anyone, including scammers, can set up a shop online under almost any name. Some online sellers falsely claim to have in-demand products, like cleaning, household, and health and medical supplies. But when you place an order, you never receive the goods. Websites often offer "medications" that supposedly can prevent one from getting sick or miraculously help an infected person recover. This 'cure' can take the form of pills, drinks, powders, and more, but cannot actually cure anyone from the virus, and just rip people off. Scammers are including "World Health Organization (WHO)" in their fraudulent schemes. Most scams including references to WHO are circulating as emails, but there are also rogue websites, as well as text messages. Many of these scams request detailed information and/or money from individuals, businesses, or non-profit organizations with the promise that they will receive funds or other benefits in return. Others ask for donations to support the treatment of sick patients or registration fees for conferences allegedly sponsored by WHO. Another type of scam proposes employment opportunities with WHO. These scams try to be more convincing by including the WHO logo, and originate from email addresses made to look like the message came from WHO or the United Nations. Scammers are also targeting victims by sending out text messages appearing to be sent from a legitimate company or organization. These messages typically include a link taking the potential victim to a site that may look real, but in reality is just a simple web page designed to gather personal information like credit card details, login credentials, and even home addresses."

—Romana Linkeova, Malware Researcher, Avast

During this global pandemic, our dependence on home internet has increased manifold as employees have set up virtual offices at home. This scenario has proven to be a golden opportunity for cybercriminals. □

A HUGE OPPORTUNITY FOR CYBERCRIMINALS

Cybercriminals are trying to exploit the Coronavirus crisis considering employees, who are working from home, an easy target

Ashok Pandey
ashokpa@cybermedia.co.in

COVID-19 has impacted many of us in multiple ways. The sudden scenario of remote working during this lockdown period has brought multiple challenges. The fragmented remote access infrastructures are very much evident now as they are only designed for 20% of an organizations' workforce.

The risks get worse due to adversaries who see this as an opportunity to steal more data and other commodities. It is an opportune time for malicious cyber attackers to exploit any gaps in our control measures to get their desired information. **Ashwin Pal, Director of Cyber Security, Asia Pacific, Unisys,**

shared the key threats emerging as a result of COVID-19: -

- **VPN allowing unnecessary access** – VPNs, by nature, allows an employee full access to resources once they have authenticated by the network. This may be ok when they are within the confines of an office environment, but may not be the case if they are working remotely. In general, 80% of employees will only need access to 20% of the infrastructure and applications.
- **Increased risk from phishing and ransomware attacks on endpoints, servers and backup infrastructure** – the volume of phishing attacks related to COVID-19 is increasing. Attackers use interest in, and concern about, COVID-19 as a means to trick users into clicking on malicious links or downloading malicious apps that are used to spread ransomware, harvest credentials, and so on.
- **Attacks on endpoints** – As more endpoints make it out into the open as a result of growing BYOD and mobility, attackers increasingly target them to exploit endpoint vulnerabilities and use them as a conduit to get a foothold into corporate environments. The big issue is that many organizations have been forced to allow BYOD due to not having sufficient laptops available to rapidly move their workforce to a remote working environment. It's these BYOD devices that are of particular concern, as they may not have the same controls in place as corporate endpoints.
- **Man in the Middle attacks** – as users increasingly work from home, their communication channels become targets. Attackers seek to intercept communications, such as via a compromised wireless access point, in order to steal critical data such as passwords.
- **Vulnerabilities at vendors and third parties** – your vendors and third parties are likely to be facing the same issues as you are. Ensure that your vendors and third parties have the necessary controls in place so as not to put themselves and your organization at risk.
- **Denial of Service attacks and hiding malicious traffic with legitimate external traffic** – Attackers can also use the increased external traffic coming into organizations as an opportunity to overwhelm your external and web infrastructure via a Denial of Service attack or hide malicious traffic amongst the increased legitimate external traffic to evade detection. This malicious traffic could be as a result of compromised endpoints or stolen credentials, which can easily go, undetected due to the rapid change to a remote working environment.
- **Inadequate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) measures** – unfortunately, a lot of organizations were unprepared for how fast COVID-19 came into play. As a result, many organizations scrambled to rapidly rollout remote working facilities. Unfortunately, this means that many put cybersecurity requirements as a secondary concern, providing opportunities for attackers to exploit potential control gaps.

ASHWIN PAL, Director of Cyber Security, Asia Pacific, Unisys

WHEN EVEN THE WORLD HEALTH ORGANIZATION WASN'T SPARED

The initial cyberattacks seen at the start of the COVID-19 crisis revolved around simple phishing techniques. The biggest victim of this was healthcare. Cyber-attacks against the World Health Organization (WHO) doubled in the last month, including a fake WHO website that mimicked the organization's internal email system

Himanshu Mhatre
&
Vivek Thawkar

COVID-19 has severely disrupted lives the world over. Measures to contain the spread of this deadly virus, including work from home mandates and restrictions on general day-to-day activities, have led to billions of people being confined to their homes. Amid the lockdown, dependence on digital channels for daily interactions and transactions has increased. This has rendered sensitive data, now accessible via a multitude of devices running on home networks, vulnerable.

With almost all operations moving from safer corporate IPs to relatively more exposed home networks, business and companies across the globe are finding it challenging to ensure security of data. Aggravating the situation, people, driven by their fear and curiosity surrounding the pandemic, have become more active on various networks, exposing systems further to lurking cyber criminals. This has taken cyberattacks to an unprecedented level.

The initial cyberattacks seen at the start of the COVID-19 crisis revolved around simple phishing techniques. Individuals were targeted with emails carrying malicious attachments appearing to have originated from genuine official sources such as healthcare authorities, and councils. Phishing-related cyberattacks rose by over 600% in March 2020. Moreover, of more than 4000 coronavirus-related domains registered globally since January 2020, 3% were malicious and 5% are dubious. More recently, cyber criminals pushed through spyware-ridden apps, playing on the general sense of fear and concern among people. Such apps, once downloaded crashed computers, locking the systems and accessing sensitive data—often users were asked to pay ransom in lieu of unlocking the systems. Cyberattacks soon moved on from individuals to targeting larger groups, such as companies in a sector.

The biggest victim of this was healthcare. Organizations in this space have reported the highest average cost of data breaches, at $6.45 million in 2019, over 60% more than the global average of all other industry sectors. Healthcare sector was naturally the primary target, given the scope for cyber criminals to exploit the anxiety surrounding the health crisis, and target individuals, healthcare setups and authorities equally.

Cyber-attacks against the World Health Organization (WHO) doubled in the last month, including a fake WHO website that mimicked the organization's internal email system. The website had been used to steal passwords and sensitive information from multiple employees in the agency.

London-based medical company Hammersmith Medicines Research, which conducts clinical trials of new medicines and vaccines, was hacked by a ransomware that accessed its patient records. Attack is believed to have been in the form of exploit kits or phishing emails containing malware.

The United States Department of Health and Human Services (HHS) faced a security breach on March 15, originating from a misinformation campaign that was spread via social media, SMS, and email. HHS's servers were overloaded with millions of requests intended at slowing the system's ability to respond. HHS was successful in deflecting the attack due to its competent security systems and multiple cyber security levels.

Several incidents were reported in other sectors as well, such as IT and BFSI.

As recently as April 18th, Cognizant Technology Solutions Corp's system network was attacked by Maze ransomware. It infected and encrypted every computer and transferred data to the attackers' server. Attackers threatened to release confidential information if the company failed to pay, in short asking for a ransom for release. The attack resulted in disruption of service for some clients.

Federal Deposit Insurance Corporation (FDIC) in the US also reported a rise in fraudulent activities in the form of fake calls, text messages, letters and emails to its customers. Scammers pretending to be FDIC employees made false claims about banks either not providing access to deposits or about security issues with bank deposits, creating panic among customers. Scammers also targeted bank accounts and other personal information of customers.

Combating cyberattacks and improving security

Organizations need to have a diverse response mechanism to manage existing and future threats. Risk management framework should be strong and effective to ensure security and continuity of business. The pillars of cybersecurity strategies and policy are:

Infrastructure with appropriate tools and controls

- Deploying appropriate multifactor authentication (MFA) for all employees in accessing networks and corporate applications according to their respective access requirements
- Ensuring virtual private networks (VPNs) are strong, and effective end-point protection systems with frequent security update cycles are in place; this would help address any vulnerability with minimum delay

- Deploying smart tools such as Intrusion Detection Systems (IDS)or Security Information and Event Management (SIEM) systems to detect potential attacks, and minimize damage

Well-defined response guidelines

- Having robust employee awareness initiatives and work from home policies
  - Ensuring that employees use only IT systems and tools provided by company and avoid using third-party devices from unknown sources; spreading awareness about the pit falls of using insecure systems/networks
  - Informing employees about security hygiene, including access control and handling of sensitive data
  - Increasing awareness via refresher training courses about typical cyberattacks, social engineering practices, and the best practices to follow in such incidents
  - Providing information on trusted sources for sensitive data
  - Building two-way communication channels between employees and security teams to ensure real-time reporting of incidents, sharing of best practices, etc.
- Monitoring high-risk users and assets to identify unusual activities or incidences that may indicate breach of protocols, or an impending cyberattack
- Providing additional front-line support to ensure necessary protocols and safeguards are in place when employees work remotely
- Testing and reworking existing incident response, business continuity and disaster recovery plans to evaluate their efficacy; having a robust emergency response plan to address and reduce, if not eliminate, risks to business continuity
- Having run books or response protocols with responsibilities clearly demarcated for security teams, business leaders, and employees in case of a cyber security incident; laying down policies to be followed in situations where critical decision makers are unavailable
- Monitoring and evaluating business systems and response mechanism of partners and third-party suppliers to as certain their capability and dependability in responding to attacks

Building cyber resilience

Persistent uncertainties demand that information security leaders across all sectors – public and private – be proactive, diligent and have a long-term vision while designing and implementing policies to ensure cyber resilience not just cyber security.

Business and information security leaders need to work together to understand likely vectors for cyberattacks emanating from vulnerabilities associated with the evolving working environment and prioritize the protection of critical information and applications. Educating employees is all the more vital, especially in case of work environment transitioning from office to home. Revamping and strengthening disaster recovery and business continuity plans is another important aspect.

In the current situation, cybersecurity companies will continue to invest in developing advanced systems and tools for accurately predicting and detecting attacks, and effectively responding on time across different working environments. Going by their experience in the current crisis, organizations would increasingly rely on advanced technologies such as AI-enabled security systems to preempt attacks and respond effectively on time. However, the growing transformation of work environment and involvement of various remote systems may mean fresh challenges for cybersecurity. As a result, cyber insurance may gain traction among organizations globally, as they look to hedge against cybercrimes.

In such a condition, striking the right balance between immediate needs and actions for long-term cyber resilience, along with risk trade-offs, will be the holy grail for business and information security leaders.

Himanshu Mhatre - Senior Consultant, &
Vivek Thawkar – Specialist, Business Research
(Technology, Media and Telecom), Aranca

NEED FOR CONFIDENTIALITY AND INTEGRITY DURING REMOTE WORKING

The increasing adoption of remote working, there is an immediate need to deploy advanced cyber-security technologies to ensure the confidentiality, integrity and non-repudiation of data

Rana Gupta

Amid the on going unprecedented global health crisis, cyber criminals are taking advantage of the situation to attack information systems across the world. With remote working on the rise, incidents of hacking are witnessing a spike as the days progress. According to a recent report by PwC, the number of cyberattacks on Indian organisations doubled in the past few days, with cybercriminals using the disruption brought about by the COVID-19 outbreak to infiltrate corporate networks and data. These cyberattacks include phishing, malicious mobile apps,ransomware and attack on insecure networks among others.

As organisations increasingly adopt remote working, there is an immediate need to deploy advanced cyber-security technologies to ensure the confidentiality, integrity and non-repudiation of data. Organisations need to ensure a working model where their workforce is collaborating in an efficient way and at the same time their critical data is also protected. Appropriate authentication and access management solutions should be in place to protect access to networks and sensitive data.

In this scenario there are certain key guidelines that organisations must follow to ensure that their sensitive cryptographic materialis stored in a secured in tamper resistant environment:

- There needs to be implementation of Smart Access Management policies along with multi-factor authentication. This combination ensures that the workforce is accessing applications and resources from the devices issued by their organisation. For this, organisationsshould look at solutions which give them combined benefits. An example of this is SafeNet Trusted Access (STA) as this gets them the Multi Factor Authentication as well as Smart Single sign-On (SSO)in a cloud based service which further allows them to deliver a range of authenticators including Grid and One-Time-Password (OTP) on the mobile phones.
- Cloud transition is a critical aspect of ensuring safety of data. Faster and higher adaption of cloud infrastructure for business applications and data is key in this situation and it is very critical to secure the cloud transition. While most cloud service providers do provide native security, organisations availing cloud services need to ensure a degree of control over the security of their own information when hosted on the cloud. This can be achieved by retaining control of the encryption keys by using Key Management solutions such as CipherTrust Cloud Key Manager, SafeNet KeySecure, among others.
- Software methods may not always work. Organisations need to ensure that they are protected against hackers causing disruption by getting inside an organisation's digital infrastructure. This can happen through social hacking like fake emails or getting unauthorized access to privileged accounts. Here, organisations can look at making sure that SSL (Secure Sockets Layer) keys are inside Hardware Security Modules (HSM). This not only provides all round safety but also safeguards the organisation's unique identity.
- Communication and collaboration among workers in a secure digital environment is important in a Work-From-Home mode. For this there are remote collaboration solutions like Citadel and Cryptobox which provide a balance between convenience and security. Both of these solutions are also already widely used by French government agencies and major enterprise customers.

While these guidelines are a prerequisite for organisations at all times, with the current crisis they become even more critical.

Apart from the responsibility of organisations, it is equally important for employees to adhere to their organisation's policies. From accessing only safe sites to safeguarding oneself from misinformation, employees need to abide by their organisation's IT security policies and ensure a safe home network. They must use social media prudently and avoid using it on business devices.

It is also important that while working from home, employees pay heed to minute details of system operation and avoid usage of any unsecured devices and unapproved tools and services. Only the IT solutions provided by the organisation that are equipped with adapted levels of security must be used.

COVID-19 has impacted businesses worldwide and changed, at least for now, the manner in which they function. Responding to COVID-19 demands that organisations think innovatively and move quickly. It is critical that organisations invest in the right technologies and systems to ensure that cyber security concerns are quickly and effectively addressed.

The author is VP India and APAC Sales, Cloud Protection and Licensing, Thales

SOCIAL DISTANCING FOR IOT—NO, YOU AREN'T PARANOID WHEN YOU SAY IT!

Corona Vaccine and Zero-day attacks, carrier-infection and IoT crowds, AI and immunity – the world of security and Corona-fighters is not too different after all. They have the same challenges, same slippery enemies and, definitely, the same monster of human-recklessness or ignorance that feeds the bigger monsters. Debasish Mukherjee, VP, Regional Sales APAC at SonicWall lets us take a peek in this petri-dish to learn how the white coats in this space are fighting the black creatures

Pratima H

Is there are corollary between how a vaccine is made and how a security solution is made for zero-day viruses and attacks? How does a security expert go about understanding a new threat and then devising a pre-emptive or corrective approach?

Vaccines are made after understanding how the virus/bacteria work and how to mitigate its threat. Similarly, zero-day attacks can be mitigated after understanding a vulnerability and how to protect against its exploitation. The newer threats like never-before-seen attacks require a much more sophisticated capability. We use AI + ML technology to recognize attacks rather than defending a known vulnerability. Never-before-seen attacks are targeted towards unknown vulnerabilities and in some cases using a system process against its own (side-channel attacks). SonicWall uses patent pending Real-Time Deep Memory Inspection (RTDMI) technology along with multi-engine sandboxing technology to mitigate never-before-seen attacks.

Can IoT pose as stark a threat for new attacks as human carriers do for Corona's contagion ability? Is there any special way to structure or place IoT devices and their adjacency (physical or virtual) to mitigate the scale?

IoT devices can pose a huge threat to any network because they are not made with security in place. Also, they are not updated for a long time or not updated at all. These legacy software present in IoT devices can be mitigated to launch an attack inside any network. Placing these IoT devices behind a robust security infrastructure and limiting its access to other network devices is the key to ensuring they are not misused for launching attacks.

Any serious or positive changes you have observed in the security landscape after the Corona crisis hit the world large?

There have been increase in attacks post the Covid-19 issue. It is seen as a result of sudden mass "Work From Home' process. Many people who were working behind a secured network suddenly started connecting from their home networks, most of which are not secured enough. In fact, SonicWall Capture Labs Threat Research Team tracked cyberattacks being deployed by opportunist hackers preying on the fear of COVID-19 Pandemic. There is a sequence to the same which we would like to share in a chronological order of their occurrence.

DEBASISH MUKHERJEE, VP, Regional Sales APAC, SonicWall

Sure. Go on.

First, there was the Malicious Archive File on February 5, 2020.In early February,it used patent-pending RTDMI to detect an archive file containing an executable file named CoronaVirus_Safety_Measures.exe. The archive is delivered to the victim's machine as an email attachment. Then came the Coronavirus-Themed Android RAT on February 26, 2020. SonicWall Capture Labs observed a coronavirus scare tactic being used in the Android ecosystem in the form of a Remote Access Trojan (RAT), which is an Android app that simply goes by the name coronavirus.

After installation and execution, this sample requests the victim to re-enter the pin/pattern on the device and steals it while repeatedly requesting for 'accessibility service' capabilities. Next came the COVID-19 Hoax Scareware on March 13, 2020: Our threat researchers observed a malware taking advantage of the COVID-19 fears- also known as 'scareware.' The sample pretends to be a ransomware by displaying a ransom note. In reality however, it does not encrypt any files. This was followed by malicious "Marketing Campaign" Propagates Android

RAT on March 14, 2020 wherein cyberattackers are creating websites that spread misinformation about coronavirus (COVID-19), falsely claiming ways to "get rid of" the novel virus. Instead, the sites attract new victims via download links.

Tell us something about the 12-Layer Azorult.Rk

It dates to March 16, 2020 and SonicWall Capture Labs threat researchers found a new sample and activity for the 'coronavirus' binary Azorult.Rk. Here, malware authors have taken advantage of the public's desire for information on the COVID-19 pandemic since it was first discovered in December 2019—and it has only escalated since. Azorult.Rk masquerades as an application providing diagnosis support, even including a screenshot of a popular interactive tool that maps COVID-19 cases and exposure. It includes 12 different layers of static and dynamic information, making it difficult for threat analysts to quickly investigate.

Any specific advice or caution for enterprises in the new paradigm of data security, business continuity and remote-working shifts?

With the need at a sudden WFH in large scale, Enterprises should be careful in choosing the right technology. The right remote access solution along with robust security technology can help them achieve the right security posture. Giving access to employees on a mass scale poses multiple challenges. A robust remote access solution that can handle load, distribute licenses on a need basis, global load-balancing and high availability etc are few important things to be taken care of. Another challenge is providing access to corporate network and sensitive data from an unsecured home network. There could be chances of a compromised home network being used for accessing the sensitive data. The secured access not only is about providing an SSL/TLS connectivity but also about proving a granular secured access.

Be aware, keep a tight vigil, communicate and have a Plan B if you want to fight Corona-time security issues

Are cloud environments at higher risks?

When multi-cloud migration occurs and companies adopt innovations, such as containers, network virtualization also needs to grow adequately in order to protect extremely complex environments ranging from public clouds to private clouds to data centers. Else, companies face blind spots of visibility and difficulties of management. Organizations must implement cloud security solutions that operate together and are easily managed like virtual firewall platforms that feature parity with its hardware firewall platform.

Dynamic and short-term spike licensing options address any unforeseen events and disaster scenarios. Secure Mobile Access enables users to leverage the economic and operational advantages of cloud platforms by launching their own virtual instances in private clouds based on VMWare or Microsoft Hyper-V, or in AWS or Microsoft Azure public cloud environments.

SonicWall addresses this new challenge with the scalability and flexibility of its Secure Mobile Access (SMA) series, which has experienced a 2,348 per cent increase of user licenses since February 2020 and adds both security and performance characteristics in its latest release.

In the latest product release, SonicWall announced that it has increased SMA 100 series capacity to support hundreds of concurrent remote users. Enterprises and MSSPs can scale upward of hundreds of thousands of users with the proven SMA 1000 series.

How can businesses bounce back without making costly mistakes on security?

Start with awareness. Just like prevention is better than cure, awareness is the key to stay secured. Be aware and vigilant, especially during times like these when cyberattacks are on the rise. Cybercriminals are opportunistic and the moment you lose the grip of security points, you might attract cyber attackers. Also, it is very crucial for an organization to ensure effective communication among its team members, leaders, customers, vendors and partners. This is one of the most important ways to deal with any disaster as well as avoid it. And, of course, just like disaster management, businesses must have plan B to be able to combat any security attack. Most businesses wait for the attack to happen and then prepare the recovery plan, which is not the right approach. Cybercriminals are re-strategizing their ways of attacks and it is imperative for organizations to prioritize and strengthen their security infrastructure.

HOW THE CRISIS IMPACTED BUSINESSES VIA CYBERATTACKS

We witnessed a substantial increase in cyber-attacks, during Covid-19 outbreak. Phishing scams and malicious software attacks have become the norm rather than exception across public offices and health care organizations. Thus, industry to work with its enterprises on being more proactive at stopping attacks in the first place, and that involves doing more than just buying and selling a cyber policy that fits the budget and thinking that addresses the risk

Ashok Pandey
ashokpa@cybermedia.co.in

In the current crisis, when the businesses have had to move swiftly to remote working for their employees, security breaches become a bigger concern. Security has taken a back seat for most organizations. As a result, solutions have been provisioned that may not line with risk exposure. Organizations are then exposed to risks that they in normal circumstances would not take.

It has been witnessed that due to COVID-19, there has been a substantial increase in cyberattacks, in the range of 14-20%. These attacks started with Phishing scams, wherein people were receiving phishing

emails, where it showed infected maps and it also asked people to download the software and then they become a victim of such attacks.

Malicious software attacks have become the norm rather than exception across public offices and health care organizations. At medical offices and hospitals, there is a huge amount of info available on patients' medical records. All these are at stake. The healthcare industry is puzzled by the sudden increase in cyber-attacks.

As per SonicWall's 2020 Threat Report, today cybercriminals are no longer interested in the size of the organization but their willingness to pay. In the current scenario, we are seeing sectors like BFSI, Education, Healthcare/ Medical being the major targets. A few case scenarios:

Medical Supply Scam: The scam campaign was targeted towards the medical supply businesses. The mail requested the medical supplier to supply the products specified in the attachment but the attached document is not a pdf file, it is a malicious executable file that belongs to the malware family Agensla. It steals credentials from the victim's browser, FTP and email clients.

Bank Payment Relief Notice Scam: This phishing campaign is targeted towards customers of Absa, an Africa-based financial services group. The mail claims to be a notice of payment relief plan for COVID-19 but the attached document is an HTML file, which when launched takes the user to the phishing webpage of Absa internet bank.

Phishing Scam: A phishing campaign from CDC, stated that it is closely monitoring the Intellectual property landscape while responding to the Covid-19 outbreak across the Asia-Pacific region. The link to COVID-19 updates in the mail is a phishing page under the veil of Spruson& Ferguson's COVID-19 website. The phishing scam has no affiliation with Spruson& Ferguson.

IRS Economic Impact Payment Scam: The malicious scam campaign involves government relief payments in America. The scam mail claims to have come from the IRS and requests the user to verify the account number in the attachment. But the attachment "Attached doc.iso" is a malicious iso file that drops a remote access trojan onto the user's machine.

Prashanth G J, CEO at TechnoBind mentioned, "the small and medium enterprises (SMEs) and multinational companies (MNCs) are suffering and in some extreme cases even shutting down. Consumers are behaving erratically, resorting to panic shopping,

PRASHANTH GJ, CEO, TechnoBind

or revising their entire values of material versus immaterial needs. The business involved in sales and production is largely affected in this pandemic."

The rise in cyber-crime in these difficult times will ensure that every business accord due importance to cyber-security.

Aiyappan Pillai, Senior Member, IEEE and Founder-Congruent Services said that "COVID-19 will make every industry review its ability to function remotely. It will bring in a new classification of businesses – those that can run critical functions in a remote way and those which cannot. While there will be functions dependent on physical presence and activities in both cases it is the level and frequency of dependency that varies. For the former, it widens the security perimeter, which means one must factor in the remote workforce as part of its security implementation and audits. The latter will look at mitigation by shifts to remote working where practical."

Covid-19 Impact on different industry verticals

IT/ITeS sector falls in the former class – Agriculture, Healthcare, Manufacturing, Transport and Energy sectors are key verticals of the latter type. They will have cybersecurity imperatives as they adopt more digital modes of working in their operations.

The Work-from-home proposition – This is going to add to cyber-security costs and efforts for individuals and organizations as the security perimeter widens depending on the geography of operations. This will be an unavoidable cost for being in business. Cybersecurity policies need to factor in personal devices and fulfilment of basic security requirements. All personal devices (mobile, PC, Tabs) need to have licensed, updated anti-virus & firewall installed and functional.

Impact on services sectors like banking and IT – The BFSI sector is in the middle of the remote vs. physical business paradigm. With digital banking already being promoted COVID-19 will give it an extra boost. Further, it is expected that the Digital economy will get a boost as it facilitates the contactless mode of transactions. A less-cash economy will push BFSI to adopt robust cyber-security measures with additional capabilities to take care of compromised customer devices accessing the systems along with that from remote-working employees. This is an existing challenge but COVID-19 is likely to amplify it.

Information & Communication Technologies (ICT) & ITES Industry, a key vertical that is keeping society functional, have a history of serving customers through remote operations. They have adapted to the new normal swiftly and will now start looking at a smaller percentage of the workforce to be physically in the company office. For e.g. TCS recently announced a plan to have only 25% of their workforce to be physically in office by 2025.

Both verticals will require cyber-security solutions for remote workers with added hardening of their central systems. A fresh wave of training of employees will be warranted to ensure the success of the cybersecurity implementations

According to Surendra Singh, Senior Director & Country Manager, Forcepoint, "Data is the lifeblood of any business, so are the employees. Recent developments have made data security more complex for organizations as they try to secure a rapidly expanding definition of the workplace. If neglected, the exponential increase in data exfiltration attempts could cause losses to the businesses."

With a fully remote workforce becoming the new way of working, managing and supporting it isn't going to be a one-time problem, which businesses must prepare for. IT leaders need to ensure large-scale remote work enablement that keeps employees productive without sacrificing security.

Organizations will need to plan to revisit decisions

AIYAPPAN PILLAI, Senior Member, IEEE and Founder, Congruent Services

on access rights, entitlements, and risk posture. At Forcepoint, we encourage organizations to see cybersecurity from a human-centric lens because the remote workforce is now the new perimeter organizations have to secure.

Rohan Vaidya, Regional Director of Sales - India, CyberArk, shared his thoughts, "the coronavirus outbreak has sent shivers down the spine of the global economy, which also affects the Indian economy to a large extent. With India locked down for more than three weeks now, the tourism and hospitality industry are affected the most. These mostly small and medium-size businesses in India employ many daily wage workers who have been out of work."

The real estate industry has been going through rough times in India and will be further affected. The commercial real estate business will see a significant disruption with many companies allowing many of their resources to work from home (WFH).

On the other hand, the movement of companies away from China to other less-developed countries could trigger a new wave of industrialization. Consequently, the expansion of India as a manufacturing hub linked with global supply chains would increase not only productivity but also create large-scale employment.

Every industry is different. Hence it is vital to understand the diverse need of these businesses and focus on specific sectors (such as pharma and automotive), which could yield greater and faster gains. These industries could be India's new play for global industry domination.

IMPACT OF FRAUD ON SERVICES SECTORS LIKE BANKING AND IT

Cybersecurity is the most critical and immediate concern for banks and financial services companies, especially, when most bank employees are handling banking application and data from an uncontrolled location, such as homes

Rajesh Kumar

In the time of uncertainty created by COVID-19, we are seeing an increase in fraudsters attempting to target businesses, andservices like banking and IT are no exception. To combat these, though the service providers are taking due precautions and effectively making required changes in the way they serve, unfortunately these are prime times for hackers to launch attacks, and one need stay vigilant.

Taking advantage of the global health crisis, cybercriminals are everyday launching new attacks and exploits, and are successful compromise users with their data and login credentials as well as able to distribute malware, trojans, backdoors for larger attacks, and even possibly resulting in ransomware.

Banks and financial services companies themselves are most vulnerable to external attacks and breaches and facing unprecedented challenges maintain requisite cybersecurity measures in line with regulatory expectations. Challenges are also emanating on how some critical and sensitive data are being handled/treated by bank's employees. While most banks have business continuity plans in place, but never tested at such large scale, especially handling banking application and data from an uncontrolled location, such as homes. While the banks are partly open as emergency services, the proportion of people require work remotely far exceeds anything envisaged while developing their contingency plans.

Further, the payment system is the most critical part of any economy and in the current times, online transactions has become integral part as well as most prevalent banking channel (be it business houses or an individual). This brings back the responsibility to the bank for any secure transaction. It is the place where transactions of various entities are at stake – be it a buyer or a merchant, or an intermediary.

Further, from the customer perspective, with every individual stuck inside their homes, people are going through anxiety and are vulnerable to making mistakes that can cost them a huge amount of money. Take for example the issue of moratorium on EMIs on housing loans. While lakhs of individuals want to avail of this opportunity provided by the RBI, cyber-criminals are using it as a chance to get people to share their personal information with them. Gullible people end up sharing their sensitive financial details and are made to click on links that immediately cost them money.

While banking is expected to be most vulnerable to these fraudsters (due to money/payments involved), the largest export industry in India, IT

Services is not an exception. The impact of Cyber is huge. This is not only due to lower billing and utilization (in wake of global lockdown). This industry may have partly mitigated by lower travel costs and other expenses, but the impact on the workforce is too large, and they not able to effectively and efficiently perform their work due to various technological and operational challenges. Further, as this involves skill-based services and every individual is driven by a different force (to logic driven, challenge/problem, collaborative working etc.), identifying employee's strength and weakness in isolation, plays a crucial role deliver productivity.

Even though, this industry always had IT-aware workforce,and this sector is all along been remote working in an onsite/off-site model, as well as have best of the BCP/DR policies in place, but still never prepared with such pandemic crisis, and mass transition on work from home. Government here in India is known to have somewhat relaxed on movement of assets to enable the remote workforce in view of the huge IT export revenues.

Most of the covid-19-related frauds have a simple modus operandi and are easily executed by taking advantage of the lack of awareness of the victim. These frauds are not new and typically extensions of common scams. Below are two most prevalent methods need to be careful. Though these examples are applicable to any services organization or industry, but most common in banking segment:

1. Phishing and Social Engineering Scams

Cybercriminals have conducted several campaigns in the last couple of months, ranging from phishing activities to distribute variety of malware. Fraudsters continue to attempt to lure victims to disclose sensitive information or click on malicious links infected with malware, leading to data compromise and fraud. Though, awareness is the key to safeguard, here are some of the guidelines or steps you can take to protect losing hard-earned money:

• Do not give sensitive information away to cold callers. Banks will never ask you for online passwords or any such information. Do not share OTP, CVVs and any personal details

• Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link, instead, delete the message.

• Do not click on links or open attachments you were not expecting to receive, or which come from an unknown sender.

• Disable the 'Auto Save' or 'Auto Complete' feature on your computers

• Before you click a link, hover over that link to observe the web address it will take you to. If you do not recognize or trust the address, re-verify. Best is to use saved links used in past.

• Be aware of bogus websites – fraudsters will often use a web address which looks almost identical to the legitimate one, e.g. 'abc.org' instead of 'abc.com'.

2. Business email compromise / impersonation of partners and suppliers

Fraudsters may call or email staff pretending to be a senior executive and request to make urgent payments. Fraudsters may be posing as suppliers and requesting payments to be made to different bank accounts details due to changes, they have had to make due to Covid-19. Further, they may pose as charities and fundraising bodies soliciting donations claiming to be involved in fighting the spread of the coronavirus. Some of the steps you can take to protect yourself:

• Independently verify any requests for new or amended bank details directly with the end-customer or supplier byusing details that you already hold on record. Be careful, Fraudsters can spoof email addresses to make them appear as though from a genuine source.

• Ensure that all your staff involved in payments are aware of this type of fraud. If they are not sure, they should not proceed before checking its legitimacy

• Always ensure your staff follow your internal procedures and controls (e.g., maker-checker) for making payments.

• If you've received one of these messages and you've clicked on the link, or you're concerned your transaction or personal details have been compromised, contact the bank immediately.

There are no technical solutions to such frauds as the criminals exploit mostly human vulnerabilities. As an IT & Security professional, we need to implement and ensure compliance for all the controls needed to make remote working safe/secure. As a Risk & Security community it is our responsibility to increase public awareness on danger of clicking onto any enticing link during these unprecedented times, and in general be extra vigilant and observant. And (finally), an ongoing risk assessment should be performed not only specific to remote access methods but as a good practice,in general.

The author is Director of Cybersecurity – Netrika Consulting India

40+ CYBERSECURITY TIPS FOR SECURE REMOTE WORKING DURING THE LOCKDOWN

At one end of the spectrum, Cybercriminals are seeking to capitalize on the widespread panic and on the other end, the low-security standards of home Wi-Fi systems, are a serious threat for the cybersecurity sector at the moment with data of millions of people at stake

Ashok Pandey
ashokpa@cybermedia.co.in

When the entire country is under lockdown and companies have had to resort to working remotely. Employees and employers have adapted to the Working from Home (WFH) culture. While WFH employees are facing the same kinds of security risks they would encounter at their normal workplace. However, they are more vulnerable to falling for scams, with agility overnight, employees who work with sensitive and confidential data are currently most susceptible to cyber threats at the moment.

It is essential at this moment to monitor baseline behaviours and any anomalous cyber activity should be looked into in real-time basis.

Measures for the enterprises to secure the infrastructure –

- Deploy technology that allows client machines access to critical servers without using the VPN. The technology currently exists that effectively creates a cloaked, cryptographic peer to peer network between the endpoints and servers freeing up the load on the VPNs while providing access based on least privilege
- Again technology exists that not only allows users access to critical applications securely but also allows granular access controls based on identities. This not only restricts access to the required application but also enforces granular role-based access controls greatly reducing the attack surface
- The same technology mentioned above cloaks endpoints and servers making them invisible to network mapped (Nmap) scans, making them very difficult to hack. This technology can also integrate with your SIEM or other security software which, upon detection of a security incident, can instruct the software to isolate

Come to terms with it

"COVID-19 teaches us varied lessons. CISOs must focus on cyber resilience to ensure their organizations can survive another bushfire or COVID-19 event. Every organization should come to terms of knowing whether they're resilient enough and start working on a plan to address the gaps exposed by COVID-19."

—Ashwin Pal, Director of Cyber Security, Asia Pacific, Unisys

Implement cloud security solutions

"There is never a 'one strategy fits all' security approach that businesses can follow. It differs with each organization. When multi-cloud migration occurs and companies adopt innovations, such as containers, network virtualization also needs to grow adequately in order to protect extremely complex environments ranging from public clouds to private clouds to data centers. Else, companies face blind spots of visibility and difficulties of management. Organizations must implement cloud security solutions that operate together and are easily managed like virtual firewall platforms that feature parity with its hardware firewall platform."

"Dynamic and short-term spike licensing options address any unforeseen events and disaster scenarios. Secure Mobile Access enables users to leverage the economic and operational advantages of cloud platforms by launching their own virtual instances in private clouds based on VMWare or Microsoft Hyper-V, or in AWS or Microsoft Azure public cloud environments."

—Debasish Mukherjee, VP, Regional Sales APAC, SonicWall

the endpoint or server preventing east-west infection.

- This software can cryptographically segregate and cloak your backup infrastructure preventing ransomware encrypting backups. These controls must be augmented by good user education about the risks of phishing, downloading malicious apps and other cybersecurity hygiene, as well as good email and web filtering technology that can prevent phishing emails and other malicious downloads
- As above, cloaked endpoints that are invisible are near impossible to hack. This is particularly important as a single mitigating control for BYOD devices that may not be as secure as corporate devices. Additional controls such as advanced malware protection, host intrusion detection systems, host firewalls and adequate patching should be implemented. Also, consider disk encryption and multifactor authentication.
- The same technology mentioned in 1-4 above will also encrypt all traffic between endpoints and servers using IPSEC VPN tunnels. The keys used are ephemeral thus removing the need for complex key management and risks around discovery and replay.
- Have an open discussion with vendors and third parties around the increased risks due to COVID-19. Ensure that they have the relevant controls in place to safeguard their data and yours. Where vendor and third-party controls are found to be lacking, access can be restricted using the
- software discussed in risks 1-5 above to specific areas of the environment, thus containing any potential intrusions
- Talk to your telcos and other providers of denial of service mitigation services to help mitigate these types of attacks. Additional investment in user and network behaviour analysis, combined with the controls discussed above, can assist with detecting malicious traffic masquerading as legitimate traffic
- A key lesson from COVID-19 is that organisations must always be resilient and a big part of this is to ensure you have a robust, up to date and well tested BCP and DRP plans.
- Just like prevention is better than cure, awareness is the key to stay secured. Be aware and vigilant, especially during times like these when cyberattacks are on the rise. Cybercriminals are opportunistic and the moment you lose the grip of security points, you might attract cyber attackers.
- An organization must ensure effective communication between your team members, leaders, customers, vendors and partners. This is one of the most important ways to deal with any disaster as well as avoid it.
- Just like disaster management, businesses must have plan B to be able to combat any security attack. Most businesses wait for the attack to happen and then prepare the recovery plan, which is not the right approach. Cybercriminals are re-strategizing their ways of attacks and organizations must prioritize and strengthen their security infrastructure.

Educate employees on security

"New technologies have made a common life simpler at the same time it has also brought a rise in cybercrime and the fact that cybercrime now permeates every facet of society showing why Cybersecurity is crucially important. It is very important to educate employees on how to secure the company data from cybersecurity attacks."

—Prashanth G J, CEO, TechnoBind

Revisit your security policies

"Security should form the foundation of a remote workforce. As working from home becomes the new normal, security teams need to revisit their security policies and redesign their digital infrastructure."

—Diwakar Dayal, MD, Tenable, India

Focus on cyber-hygiene

"At this juncture, more people are working remote, the security perimeter can practically be assumed to be global. Hence it is equally important for both organizations and individuals to take adequate steps to secure their respective ICT infrastructure. The recommended steps focus on basic cyber-hygiene as well as behavioural aspects. The success of cybersecurity measures is dependent on correct end-user behaviour and hence is an equally important aspect to be addressed."

—Aiyappan Pillai, Senior Member, IEEE and Founder-Congruent Services

- Streamline and standardize the technical processes to help employees work efficiently, regardless of their location or device.
- Use resources such as cloud-based services to foster agility and enable employees to easily and securely access the apps and data they need.
- Restrict access to business networks by allowing only authorised access to data and business resources.
- Use Software-as-a-Service (SaaS) collaboration tools to facilitate online interaction and communication.
- Regularly communicate with internal and external stakeholders to look for ways to improve productivity and security.
- Stay informed of the evolving threat landscape to adapt and respond quickly.
- There has been an increase in phishing attacks over the past few months, especially on work emails. As more people work-from-home, hackers are leveraging the current scare and panic to make most of the situation. Security leaders must ensure that their employees are updated on different types of attacks or ways a phishing attack can take place — not just over email but also over other channels like phone calls or online chat.
- All employees should have two-factor authentication for any company logins, be it internal applications or SaaS-delivered ones, ensuring that only the right people are accessing certain sensitive data as well as to reduce the risk of password sharing.
- There have been countless incidents from unknown USB drives infected with malware. Unsanctioned data movements will be on the rise due to work-from-home and people will have to sometimes be "creative" on how to transfer data to get their work done. Make sure you have updated antivirus software and use trusted and encrypted USB keys if possible.
- Once a hacker, criminal organization or nation-state has gained access to this sensitive information, it's incredibly difficult to regain control of it. When you need to transfer critical or confidential data, take a few seconds to pause and reflect: can I move this data to this new location? Is the new location safe and sanctioned? Will, the data-in-transit be protected by my VPN or other encryption means.

From an organization perspective, the following steps are recommended

- Ensure Passwords for access and control with robust policies and strict enforcement
- Firewalls and Anti-virus to be updated with IDS, IPS, DDoS, APT protection capabilities among others
- Harden all servers whether physical or in the cloud. Those operating through cloud service providers need to ensure the same rigour
- Encryption policies and mechanisms for removable media
- Ensure aggressive logging and monitoring. Follow up on every suspicious activity. Better to be safe than sorry
- Implement Multi-factor Authentication (MFA)
- Avoid the use of notified collaboration platforms that pose cyber threats. Regularly refer to www.cert-in.org.in for notifications
- Security procedures and compliance mandates to be circulated to all employees. This is partially elaborated in the next part.
- Conduct regular cybersecurity awareness and practice training

Tips for employees to act responsibly

- Ensure Passwords for access and control
- Employees should be encouraged to log out from the corporate network at the end of every day.
- Ensure that personal devices have firewalls and anti-virus software installed, kept update and always on. It should also be enabled to protect any browser
- Avoid the use of notified collaboration platforms that pose cyber threats.
- Use collaboration tools with built-in security controls for access and audit.
- Equip your IT support staff with robust and secure remote support tools.
- Regularly refer to www.cert-in.org.in for cyber-crime related notifications
- Undergo regular cybersecurity awareness and practice training
- Never use – freeware solutions even from leading solution providers. Always go in for the best in class solutions even if it is a paid option.
- One should change their default settings and passwords to reduce the potential impact on their work of an attack via other connected devices.
- Employees working remotely should be required to use multifactor authentication (MFA) to access networks and critical applications.
- A virtual desktop interface solution is also a good solution.
- To avoid risk, one should turn off any file-sharing on the work system and ensure home router or Wi-Fi access point has WPA2 security enabled while accessing or working on an important document.
- Follow all mandated security procedures and practise basic cyber-hygiene such as
  a. Setting strong passwords with a mix of the lower and upper-case alphabet, special characters and numerals
  b. Passwords should not include known generally details from one's personal information
  c. Keep different credentials for different applications
  d. Change passwords periodically
  e. Never store the passwords in an easily accessible location
  f. Password-protect documents
  g. Log out/ close session as soon as the activity is complete
  h. Do not click on emails or attachments from unknown sources
  i. Make context-aware decisions when dealing with known sources
  j. A primary behavioural trait that needs to be inculcated is not to take anything at face value. Verify all information or transaction. Err on the side of caution, though it may seem delicate or awkward, just like how one goes through a verification process on call or in person.

Practice daily vigilance

"Businesses never planned for security and business continuity strategies for kind of situation we're in currently. Even if they had, it wasn't the part of the overall security program for 100 per cent remote workforce.

Under an extended period of stress, anxiety and desperation can make it easy to let one's guard down when it comes to online threats. Businesses and individuals must practice security vigilance daily and always consider the authenticity of emails.

To ensure safe collaboration among the distributed workforce, businesses need to adopt security measures, and security leaders must engage with employees working remotely to encourage them to practice active security hygiene."

—Surendra Singh, Senior Director & Country Manager, Forcepoint

It must be understood that cybersecurity solutions are not just for large organizations but are required for all. It is not a luxury but part of basic hygiene. As seen from above, the end-user plays a major role as a potential gateway for cybercrime. Hence, to sum up, it is apt to say that even with standard cybersecurity solutions in place, to avoid getting infected, one must make conscious efforts to stay safe both in the real and virtual worlds!

THE ROLE OF THE CHIEF DATA OFFICER IN NAVIGATING THE CRISIS

The Chief Data Officer (CDO) of each sector and industry can minimize the impact of the pandemic on the economy by taking well-informed and data-based decisions

YogitaTulsiani

The COVID-19 pandemic has created tremendous pressure on the economy of every country it has hit. It has had an extraordinary impact on businesses and the livelihood of individuals. As the spread of the virus shows no signs of slowing down across the globe, governments of almost every impacted country are taking unprecedented but informed steps to keep their citizens safe.

Which sectors require CDOs?

The only way to keep the citizens safe and minimize the impact of the pandemic on the economy of a country is by taking well-informed and data-based decisions. It is the responsibility of the Chief Data Officer (CDO) of each sector and industry to sift through real-time data for deploying appropriate crisis response. CDOs play critical roles in the decision making in almost every industry including –

i. *Healthcare* – based on information from the CDOs the hospitals and specialized care units can prepare PPEs, masks, beds and ventilators for the influx of patients.

ii. *Grocery chains* – depending on the real-time demand of food and essential items, grocery chains and (online) delivery services can stock up on the necessities by predicting the incoming orders from people.

iii. *Telecom* – as more people work remotely, telecom companies need the help of their CDOs to upgrade their services where there is a high demand for network traffic data.

How are CDOs contributing to the informed decision making of their organizations?

There are three main categories of actions CDOs must undertake to guide their organizations or companies successfully through the crisis and prepare their companies for the new normal that lies ahead of the pandemic –

Ensuring that the business/organization remains operational

i. Continuing the business operations

Continuing business operations rely upon the informed decision making of the board of directors (BOD). It is the CDOs responsibility to make sure that they collect and analyse real-time data from reliable sources.

Apart from ensuring the continued safety of the other employees, CDOs should maintain flexibility to revisit the core data platforms to ascertain reliability and authenticity.

ii. Setting up a data-nerve centre

A dedicated COVID-19 data-nerve team can work remotely, but the team should always include data engineers, data scientists, report owners, data stewards and data-visualization specialists.

A data-nerve centre for a COVID-19 impacted business collects the correct input, process it in a way that is understandable for the BOD and to set up potential information-driven reactions to situations.

It should work closely with the COVID-19 response team at the enterprise level and drive rapid actions including the development of executive dashboards and company performance reports.

iii. Maintaining data safety and privacy

The organizations that are collecting bulk volumes of data need to ensure that their firewalls are up and running, but they also need a round-the-clock monitoring system.

CDOs much work in coordination with the company IT and security team to ensure the maximum safety of the company data, which includes limiting the access of remote workers and allowing only specific devices to access company profiles.

Bring profitable flexibility to company operations for oncoming challenges

i. Chalk out plans for high-stress scenarios

CDOs need to collaborate with the company's planning and strategy team to identify the possible high-stress scenarios arising from the effects of the COVID-19 pandemic.

They must also adjust data sources and processes for adapting to the multiple challenges that may arise during these high-octane situations.

It might involve switching to new sources of data and adopting new data processing workflows to guide the decision making machinery of the company.

ii. Find ways to reduce cost

Companies must reduce their operational cost during situations of high-stress. CDOs need to collect investing data and work with the CFOs to reprioritize their resource allocations and invest in new, more secure opportunities.

Information from the CDOs can help the CFO and his team to reduce company expenses and simplify their portfolios in the face of prolonged health and economic crisis.

Planning and preparing for the post-COVID-19 days

i. Seek future investment opportunities

The information provided by the CDO can contribute to building a 360-degree consumer portfolio. That can provide the finance team with new windows of opportunity for more profitable investments.

Companies are already making it a practice to base their investment decisions largely on real-time information provided by their data officer and his/her team. It is paving the path for smarter investment initiatives by the company that will take care of long-term goals in the future.

YOGITA TULSIANI, MD & Co-founder, iXceed Solutions

ii. Building a crisis plan

Most companies had no crisis plan when COVID-19 hit and they are currently developing one as they work in the COVID-19 ravaged economy.

CDOs can work with the CFOs, CEOs and other CxOs to develop a crisis plan that they can instantly deploy in the future during a similar global crisis.

iii. Digitize majority of the workflow

Remote working has set new precedence and it has helped several organizations cut office-maintenance costs.

It can become the future of work for innumerable teams and brands, if the CIOs can collect, process and retain operational data from this period and present it during the new normal.

While the pandemic has made it difficult for almost every individual and company, it has also taught most organizations that adaptability is the key to survival. With a little help from the CDOs, the company employees can remain safe and yet work remotely. And it is certainly practical to hope that this period will reinforce the importance of data safety and the ethical use of information.

The author is MD & Co-founder, iXceed Solutions

HOW BANKS AND FINTECH COMPANIES CAN HOLD THE ECONOMIC FORT TOGETHER

Recently, a UK based FinTech company came up with a tool to assist businesses in securing loans based on their past incomes as a collateral. Once fully operational, this tool could be a great support for smaller businesses to stabilize their revenues and keep afloat in these uncertain times

Hozefa Muchhala

The phrase, "When the going gets tough, the tough get going" holds true now more than ever; and testimony to this are several FinTech companies that are stepping up to the ongoing global health crisis and brainstorming innovative solutions within the confines of their homes.

The virus is moving at a rapid pace and whilst the government is rolling out several initiatives and funds to support the masses, it cannot be denied that SMEs and MSMEs are facing the brunt of the economic downfall. Without strategic support from larger financial entities, these businesses will not be able to survive the storm for long.

Two sides of the same coin

The past year had already promised greater collaboration between banking and FinTech firms with the aim of quality solutions for customers. This year, as we enter the second quarter with anomalous

challenges hovering over the global and national economy alike, banks and NBFCs need to come together to innovate and create relevant solutions for people and enterprises while addressing liquidity and credit concerns at the grassroots level.

Banks have worked relentlessly over the past 20 years to produce sticky solutions for business and customers. However, a lot of traditional banks that want to deploy and lend funds, are willing to do so but are not operationally equipped for the same as they are used to lending in a more traditional mechanism. They are getting overwhelmed by loan requests from small businesses. Thankfully, FinTech companies are built with technologies that can help approve loan applications in a much faster manner, scale accordingly and get money to where it's needed the most.

Several companies are already addressing key hurdles faced by enterprises when it comes to business lending. FinTech companies have also extended support to banks in loan application assessments and disbursements. They are modifying their offerings to accommodate needs of banking companies that want to connect to businesses and distribute funds with their existing capacities. These are great examples of how FinTech inventions, if supported adequately by concrete banking tools, can help with some of the most difficult challenges faced by the government.

An important time for FinTech

FinTech innovators are capable of reaching out to those parts of the economies that were relatively untouched by banks; being too small or risky or areas wherein banks are uncomfortable to operate. This enables them to serve a broader digital economy. The role of FinTech firms is key in the current scenario because they can easily adapt to new environments and technologies. Global FinTech companies offering diverse solutions from procurement services, digital payment tools and digital lending technology have stepped forward and vouched to protect economies from a possible wave of bankruptcies, by extending faster payments to people and businesses.

Further, as the WHO encourages contactless payments, many businesses are moving towards digital payments for transactions to prevent the spread of infection. This dependence on digital banking is a great opportunity for FinTech firms to bring enhanced solutions to the table. Although this increases the proportion of digital transactions, there has been an evident overall reduction in payments across the country due to reduced spending, leading to lower profitability for firms. Additionally, with people being inclined to invest more 'safely', investments in risky early-stage FinTech startups are slowing down. In such times, the collaboration of FinTech with traditional banks could really be a win-win for both.

The Way Forward

Unprecedented crises like these demand competitive solutions to meet distinguished consumption needs. The future will require us to reconfigure value chains for financial services across the board and pick up from distressed times, strategizing for a new tomorrow.

Empowering organizations by AI and cloud computing, FinTech companies are helping organizations to derive macro business insights on a real time basis and assisting them to make informed decisions in these testing times. On the other hand, banks need to be more involved with FinTech innovators by allowing them to discover more on the UI/UX space and backing them with improved core banking functionalities. As banks hold on to their customer based models and gradually progress on the principal banking front, they must partner with technology innovators that have lesser resource requirements for quicker, better and futuristic outputs. This will enable FinTech players to produce need-based services for businesses and customers with better revenue modeling for both. Also, they will benefit from solid financial systems of banks and a larger business/ customer base to interact with.

Since FinTech players are not bound by the shackles of traditional restrictions, they can help other sectors to emerge from these crises. Emergence of alternative credit platforms and innovative business models are set to shape the lending space and drive financial inclusion. At this time, beneficial partnerships across industries including telecom, e-wallets, banks and similar can contribute to meeting evolving needs. An entity's capacity to innovate will dictate the path ahead for it. Decisions have to be made dynamically and aggressively. Collaborations between banks and NBFCs can indeed step up and assist governments to protect economies, rather than functioning independently or in competitive space. It is essential that the government extends sufficient support to FinTech partnerships to unearth their true democratic potential.

The author is Founder and CEO, Ginger Root Code Factory

WHEN THE WORLD WENT VIRTUAL OVERNIGHT

Major shifts and disruptions in the workplace due to COVID-19 can lead to critical gaps in the employee experience and have serious implications on employee well-being, productivity, and the long-term business, if not addressed quickly, feels Anand Raisinghani, Vice President, Platforms & Technologies, SAP Indian Subcontinent

Sunil Rajguru
sunilr@cybermedia.co.in

How are you coping with the current Covid-19 crisis?What are your tips for enterprises?

The world went virtual overnight and had to change their processes and strategies to suit the new reality. We are no different. While we are now getting accustomed to the new reality of remote working, technology has helped us stay connected. We have leveraged the power of technology to help us carry out our business seamlessly not just for our employees, but in strengthening our engagement with the customers.

I believe the key lies in building seamless engagement platform with employees and communities we live in. We want to make the best use of this time to offer our stakeholders—be it customer, employees or partners with multiple opportunities to learn and upskill, reskill themselves. Various online sessions, workshops, webinars, etc. has helped SAP to enable its workforce and enterprises could adopt this approach to keep the employees motivated and satisfied

This global pandemic is an opportunity for

enterprises to adapt and explore digital tools faster. Businesses should ensure that they focus their efforts on connecting with customers beyond just transactions. While customers too are learning to adapt to the change, it is imperative for organisations such as ours to support them through this journey. In addition to this, engaging with partners is more important than ever at this juncture. We are skilling our partners and customers proactively along with sharing tips and tricks with our peers in the industry to overcome this hurdle.

What changes do you see taking place in technology in a post-Covid-19 world?

The post-COVID era is going to offer a new perspective to a lot of ways in which the world was functioning—a stronger synergy between system, people and processes. People will be more digitally equipped, teams would be more collaborative and there would be a positive sentiment between groups. Technology that is binding us together now, will take a more important role in the lives of people and organisations. The importance of technologies like cloud, AI, machine learning, etc. are going to come to the forefront since organisations today have experienced the benefits of it first-hand.

The focus of businesses will be to ramp up volumes and get back to normalcy. It is also going to be culturally challenging, but we must take it as an opportunity for teams to stay motivated, learn new skills, new business models by leveraging digital technology and conducting knowledge sharing sessions and come back stronger than ever.

Specifically, how will ERP evolve beyond 2020?

The aim of organisations will be to get back to normal as soon as possible and hence every decision made will have data backing it up. Right from supply chain to management to purchasing management, ERP is going to define the productivity of organisations in the immediate future. With cloud ERP solutions leading the way, personalised ERP solutions are going to be in demand to recover quickly from the economic impact. We are also hoping to see a rise in adoption of ERP solutions by SME's in order to enhance their processes and productivity.

As enterprises emerge from the COVID-19 crisis and seek to reduce operational risk while enhancing digital capabilities, migration to S/4 HANA can be an opportunity to adopt newer, more resilient cloud-based technologies that can help to achieve those objectives.

How do you address the massive disruptions in the global supply chain?

Global supply chains have been disrupted in the past few months, across industries. It is becoming increasingly important for organisations to protect their supply chain operations by undertaking measures like focusing on extended supply networks, exploring alternative supply chains and scenario planning. SAP operations are supported by several strategic suppliers. We are with them in this journey to ensure they apply comparable mitigation practices with their teams, while maintaining superior service levels.

Our customers and partners are an integral part of SAP family and we are doing our best to ensure their business continuity by providing access to some of business-critical SAP solutions:

- **SAP Ariba Discovery** – offer both suppliers and buyers an open platform to post and solve their sourcing needs.
- **SAP Qualtrics** - Opened the XM Platform to create a free Remote Work Pulse thereby enabling organizations to manage and support their employees. This include understanding their requirements and how they can help their employees feel supported and productive
- **TripIt from Concur** - Offering services to organizations help with travel issues
- **SAP Litmos** - Providing remote training capability

How has the Qualtrics Remote+ On-site Work Pulse benefited the new WFH reality?

Major shifts and disruptions in the workplace due to COVID-19 can lead to critical gaps in the employee experience and have serious implications on employee well-being, productivity, and the long-term business, if not addressed quickly. Toadapt to the new WFH realityeffectively, we are offering Remote Work Pulse. Remote+ On-site Work Pulse is a technology offering from SAP Qualtrics to help organizations assess preparedness for a remote workforce and is publicly available for free.

Organizations making use of the Experience Management (XM) platform can rapidly address entire workforce needs around well-being, safety, resources, and enablement for their employees working from home. Theyofferorganizations with surveys and corresponding reports to quickly identify and prioritize employee needs in order to take quick actions.

5 smart products we could do with right now!

Sunil Rajguru
sunilr@cybermedia.co.in

Every generational shift brings its own bouquet of products. The desktop, the Internet, the smartphone: They all spawned their own industries. The Covid-19 crisis is such a generational game changer. Many new products will come as a result of it in the future and here's a looking at some that could be quite handy

1. Transparent Bluetooth masks: People are talking of having a lockdown for 3 months, 6 months and there are even some wild demands for having it till 2022. Plus Covid-19 is actually SARS 2 and a Coronavirus can mutate every month. So, pandemic scares could be the new normal. People wearing masks all the time is dangerous (identity issues and theft could become easy) and irritating. This could easily be addressed with transparent Bluetooth masks. They would still allow you to still see the features of the other person's face. They would keep you in touch with your mobiles. The mask could have sensors that detect body temperature and other factors that to know if you are well or not.

2. Super IoT health bands: IoT wearable health bands can already detect body motion, heart rates and form some sort of ECG monitor. In the future they could be re-engineered to test your moods, stress levels and even analyse your sweat. They might be able to detect the air quality around you (with relation to pollutants and pathogens) and alert you. You could have a GPS air map which tells you about the quality of air that you are headed for. These details could be alerted to your family and your local doctor/hospital if you should so desire. This could be connected to your Bluetooth mask.

3. Home testing med kits: Defunct medical startup Theranos said that they had "devised blood tests that needed only very small amounts of blood and could be performed very rapidly using small automated devices". Unluckily that turned out to be a fraud. But it still can be done. It's theoretically possible and now the world, the medical industry and scientific research community has the will to do so—fast! We could well have a spate of med startups now that could deliver it. Just do a basic test at home to know if you're in the red or not and no need to go to the hospital.

4. Super monitoring apps: One smart alec quipped that privacy works only if either everyone has privacy or no-one has. We know the governments of the world are monitoring our every move. We just demand that we get it in the form of Big Data. From now on governments will be monitoring the populace and checking for things like disease spikes in any part of the world. Well, all they have to do is share that Big Data in real time to the consumers. The concept of red, orange and green zones could be made permanent and updated in real time. They could also include war zones and include natural disasters.

5. The return of Google Glass: In the era of social distancing and the need for more information immediately about your surroundings, it's high time that Google Glass made a comeback. We all seem to be destined to be loners when we walk out into the streets. What if we combined all of the above? A glass mask that incorporated protection against pathogens, Bluetooth-enabled, with a Google Glass type interface, connected with your IoT band and with access to all the global real-time apps? Now that would really be something!

INDIAN DRONE STARTUPS TURN THEMSELVES INTO FORCE MULTIPLIERS DURING LOCKDOWN

Indian drone startups are now acting as force multipliers for the municipal bodies and the police forces. During the lockdown, we have seen them exploring new and innovative ways drone tech can be used in battling the ongoing crisis—by doing surveillance, detecting infections, disinfecting areas, delivering medical supplies and so on

Soma Tah
somat@cybermedia.co.in

The conversations about the promises of drone technologies have never been more relevant, especially at a time when governments and local authorities around the world are scrambling for ways to combat and contain the spread of the Coronavirus and that too with minimum human interactions possible. Because the frontline workers who are working tirelessly to safeguard people are at greatest risk of exposure to the infection and if not protected, they can become the vectors of further infection as well.

Drones have proved to be particularly useful

in aiding government efforts to curb the spread of the disease, because they can reach areas that are difficult to cover either by foot or by vehicles and can do it much faster. A drone can cover a distance of 10km in just 8 mins. Another advantage is that it keeps frontline workers away from close contact with potentially infected people.

There are few basic ways in which drones can and are being used right now:

Surveillance and enforce lockdown measures

Drones are now being used for real-time surveillance of public places in major cities and to help local authorities enforce lockdown measures effectively, without deploying any on-ground personnel.

Regular surveillance using drones also acts as a strong deterrent against lockdown violations. A drone carrying an HD camera and a megaphone can be used to disperse gatherings and canvass precautionary messages, such as to put on your mask or maintain social distancing, etc.

Spraying disinfectants to sanitise places

Crop spraying drones can be utilized to disinfect public areas more efficiently without causing any health hazards. The speed and area covered in the process are unmatched. Disinfectants spraying drones with a 16L tank can sanitise 100,000 square meters in an hour. The spraying activity does not take more than just 2-3 minute and can be repeated as many times as necessary.

Many city municipal corporations have already resorted to this hassle-free surface disinfection technique to sanitize crowded marketplaces, railway stations, areas around hospitals, garbage dumps, etc. If needed, these drones can be used effectively for air disinfection also.

DJI Agras MG-1 spray drone

Check infection with thermal imaging

Drones with thermal imaging cameras can detect high body temperatures from a distance of around 10 ft away. The data can be analyzed further to understand the level of infection in certain areas and to help authorities to take necessary actions.

A public canvassing system can also be used alongside to monitor highly infected zones and give appropriate instructions to the people.

Medical supplies delivery

Drones have also proved to be an efficient means to deliver critical medical supplies in emergency scenarios. They can deliver first aid quicker than traditional ambulances. Not only does it help in

Aquiline Drones

speeding up deliveries of essential medical supplies, but also reduce the exposure of medical staff in a pandemic like situation. Most drones can be easily modified with a payload drop mechanism to deliver packages up to 6 kgs.

Indian drone startups step up to help cities tackle the crisis

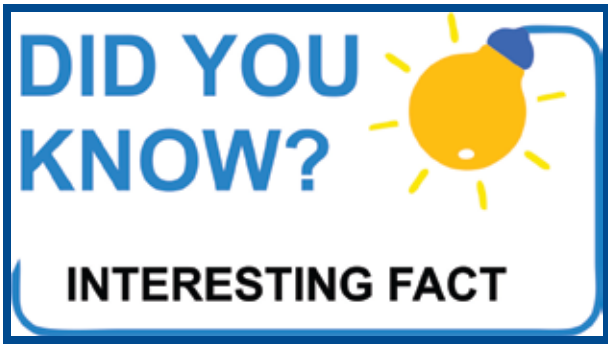
In this ongoing battle against the Coronavirus crisis, a bunch of Indian drone startups are now acting as force multipliers for the municipal bodies and the police forces. During the lockdown, we have seen them exploring new and innovative ways drone tech can be used in battling the ongoing crisis -by doing surveillance, detecting infections, disinfecting areas, delivering medical supplies and so on.

City authorities and police forces have also embraced these solutions for strategic and targeted jobs. For instance, police forces in Sangli and Guwahati have turned to drone-maker, ideaForge to enforce lockdown measures. The dronemaker has partnered with Fractal Analytics to offer AI-powered drone solutions for real-time and intelligent aerial surveillance.

New Town Kolkata Development Authority (NKDA) chairman Debashis Sen said, "We are using drones to disperse any gatherings that violate the social distancing guidelines. Marketplaces and adjacent roads often tend to get crowded during the morning and evening rush hours. Hence, we are using drones to closely monitor those public places. We are also considering using drones for sanitizing areas."

Bengaluru-based drone company, General Aeronautics, which has expertise in precision agriculture, and in emergency medical delivery including transportation of active blood control kits and organs for transplantation is now helping municipal corporations in the cities such as Bangalore, Mysore, Bhubaneswar, and Cuttack to sanitize those cities using drones. It is also working in tandem with the respective police forces to carry out disease surveillance tasks in those cities.

The drone company is also working on to create a crowdsourced drone surveillance solution model for the Bangalore City Police by pooling the drone enthusiasts, events and wedding photographers in the city. Abhishek Burman, founder director and CEO, General Aeronautics, said, "Around 80-100 drones can be easily pooled this way in Bangalore now for such a crowdsourced solution. The solution we are designing will help integrate live camera feeds generated by all these drone operators to a command and control



Drone Tidbits

'Drones' or 'Unmanned Aerial Vehicles' (UAVs) are purpose-built pilotless aircraft that can be controlled remotely or can be autonomous with a combination of technologies, including computer vision, artificial intelligence, object avoidance tech, among others.

Consumers' interest in Drones have grown exponentially in the last years, but their roots date back to the first World War, in the early 1900s, and usages were originally focused on military purposes only.

Drones can be as large as an aircraft or as tiny as a hummingbird and can be flown varying distances and heights, and that's the reason that they are capable of carrying out some of the complex jobs in the areas, which are hard to access for humans.

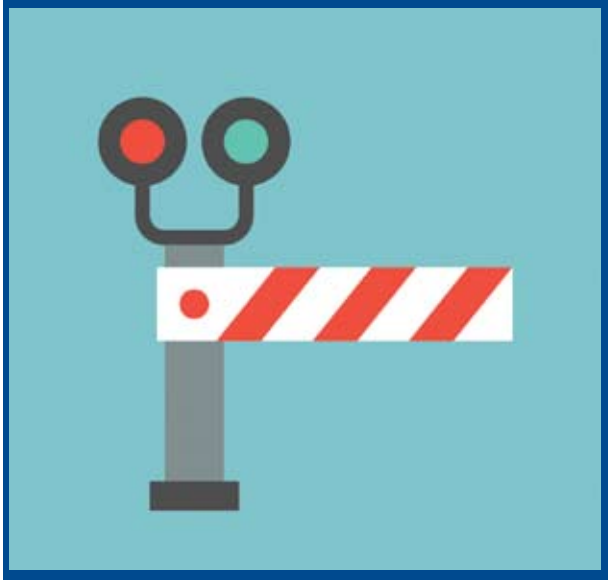
There are 4 broad drone variants based on the type of aerial platform used: Multi Rotor Drones, Fixed Wing Drone, Single Rotor Helicopter, and Fixed Wing Hybrid VTOL.

Mini drones are the best drones for beginners, because they are small, affordable, and easy to fly, while sophisticated drones are being used for more targeted jobs like aerial photography, surveillance, commercial delivery, disaster and emergency response, etc.

Drones have very low battery life. Most drones can stay in the air for 10 to 30 minutes only. The flight ranges vary from 80m to 7km. Battery recharging times can be as frustrating as short flight times. It may take 50 minutes to as long as 3 hours to fully charge.

The longest drone flight recorded so far is for 4.4 hours by a Quaternium's HYBRiX.20 fuel-electric quadcopter that uses a mixture of gas and electricity for power.

India's Drone Woes:



Outdated policy: India is still awaiting Drone Regulations 2.0.

Regulatory bottlenecks: Flying a drone in India is not as simple as buying it. The NPNT Compliance, the complex Digital Sky platform have added to the woes further.

Illegal flying: Many drones are imported illegally, and continue to fly illegally.

Hugely varying costs: Locally-made drones are often way too expensive (10-20x higher) than the imported ones. Prices of the solutions also vary widely.

centre for monitoring, analyzing and creating alerts. Every single drone operator will be assigned to one police station for compliance reasons."

Another Delhi-based drone startup, Indian Robotics Solutions has developed a Corona Combat Drone that is transformable and can accommodate a medicine box to carry essentials like portable corona testing kits and medicines, spotlight for night utility, speaker for giving instructions and a disinfectant tank in addition to a thermal imaging camera.

"If we find a person who has high temp, he/she can be identified and taken away by the authority and the area around him can be sanitised accordingly through the same drone. We are in talks with various state governments as well as the central Govt. for its deployment specifically in the red zones," said Prashant Pillai, Co-Founder, Indian Robotics Solutions.

The startup is already working with North Delhi Municipal Corporations (NDMC) for sanitizing the area and is also in talks with various state governments as well as the central government for their Thermal Imaging drone.

Another Indian drone startup, Marut Dronetech is already conducting trial runs with state governments of Telangana and Andhra Pradesh and Trichy Municipal Corporation for its Thermal Imaging drones. The drones are fitted with infrared cameras and can be used for thermal screening of groups and to identify suspected cases at an early stage.

Will drones become mainstream in the post-pandemic world?

The pandemic has opened doors for many drone operators to go mainstream with their unique offerings. Many such offerings are likely to find sustained usage scenarios in the post-pandemic world as well.

Sukanya Mandal, IEEE Member feels that the post-pandemic world will see increased use of drones for supplying the much needed daily essentials or the emergency medicine to villages or remote areas that are difficult to reach by roads. Agricultural drones will also become mainstream.

Glenford V. D'Souza, Senior General Manager, LYNX: Lawrence & Mayo feels that drones will become part and parcel of households and industries over time. "We can confidently expect a significant increase in the use of drones due to its versatility and multi-purpose applications. Additionally, several other applications are currently being invented to make this even more dynamic," he said.

Vipul Singh, Co-founder and CEO, Aarav Unmanned Systems said, "I believe the regulations will be operationalized very fast now to make it easy for our police forces to adopt drones surveillance and crowd management in the post-pandemic world."

Ankit Mehta, CEO of ideaForge said, "The COVID-19 pandemic has shown us that our current resources and strategies may not be adequate in mitigating crises like these in the future. We must augment and strengthen our security and surveillance framework with drone technology as it will enable the authorities to take control of a situation. The administration has realized this need and has shown an increasing interest in procuring drones."

THINGS TO KNOW BEFORE FLYING DRONES IN INDIA

Flying drones is legal in India and the government has set up some drone flying guidelinesin 2018 along with 'Digital Sky'—a single-window online platform to handle applications and issue flying permits for commercial usage

Soma Tah
somat@cybermedia.co.in

Know the Drone categories:

Nano: Less than or equal to 250gm
Micro: From 250gm to 2kg
Small: From 2kg to 25kg
Medium: From 25kg to 150kg
Large: More than 150kg

A permit is required for commercial drone operations (except for those in the Nano category flown below 50ft and those in the Micro category flown below 200ft).

Know Drone flying zones:

Red Zone: Flying not permitted in areas near airports, international borders, Vijay Chowk in Delhi, State Secretariat Complex in State Capitals, strategic locations, and military installations, etc.

Yellow Zone: Permission required before flying
Green Zone: Automatic permission is granted

Know the Dos and Don'ts:

- Every drone operator will have to undergo training at a DGCA-approved flying training organization (FTO). Pilots must be 18 years of age and should have studied up to a minimum of class 10 in English.
- Drone operators must follow Civil Aviation Requirements (CAR) issued by DGCA,whether in controlled or independent air spaces.
- A Unique Identification Number (UIN), which is similar to a license plate is required for all drones, except for those in the Nano category.
- Additionally, operators require an Unmanned Aerial Operator Permit (UAOP) or a Remote Pilot license if flying the drone above 200ft.
- Obtain necessary permissions before every single flight. Inform the local police 24 hours before starting drone operations.
- Foreigners are currently not allowed to fly drones in India. For commercial purposes, they need to lease the drone to an Indian entity who in turn will have to obtain a UIN and UAOP from DGCA.
- Follow airspace restrictions and no drone zones
- Fly only during day time.
- Fly in visual line of sight. Drones cannot be flown more than 400ft vertically.
- Operators risk cancellations or suspension of the UIN/UAOP if any of the government regulations are violated and will face penal action under the relevant IPC sections 287, 336, 337, 338, Aircraft Act 194, and Aircraft Rules.

25 COOL THINGS YOU CAN DO WITH DRONES

Drones have been getting better and better in the last few years and are now very versatile. All the big tech companies are trying to figure out how to optimize them. The only thing that has been holding drones back is regulation. With the lockdown scenario as a result of the Covid-19 pandemic crisis and the focus on no touch technologies for the future, this is one thing that could take off

Sunil Rajguru
sunilr@cybermedia.co.in

1. Spray disinfectant during Covid-19: All over the world, drones are spraying disinfectants in public places to keep zones sanitized. The same is the case with India. After the crisis is over, will drones take over the spraying of things like DDT too?

2. Deliver regular stuff: Potentially this is huge. BigBasket, Amazon, Swiggy, all have really mushroomed and the delivery boy network had reached unprecedented levels. Initially probably the larger orders and those at remote places can be handled by drones. Could they do it 100% in the future?

3. Deliver in hazardous zones: This is quite useful during earthquakes and floods when roads are out and helicopters and boats are limited and can be used sparingly. Drones can deliver medical emergency kits, food and get back valuable information for disaster planners.

4. Surveillance: This will be popular for governments: national, State and local; also for espionage. Corporates can also keep track of their large properties. This is becoming easier with increasing bandwidth speeds and data centre storage.

5. Aerial photography: Nothing says bird's eye view like a drone. But it can also be used for underground tunnels, skimming the surface of water and generally getting into areas where it's difficult for the human hand or camera to reach.

6. Film shooting: While the lockdown will end for the normal people, what about large gatherings? Film shoots may have hundreds of people and so the risk of infection is high. What if films came out with very less actors being shot by drones with cameras controlled from a remote location?

7. 3D mapping: Surveillance and aerial photography is fine, but what if you wanted to make a 3D map of an area? People like Albert Lin have been doing this for their documentaries for quite some time now and it is also useful for city planning.

8. Use in war zones: The military is usually ahead in using cutting edge technology and drones are no different. One person even managed to put an AK-47 a drone and make it work perfectly. They can also be used to neutralizing mines.

9. Racing: Drone racing is awesome thanks to the in-built camera plus the fact that the drone can go high or even appear to be hugging the ground. With large spectator sports under a cloud could we have the World Drone Championships in 2021?

10. Chatbot drones: What if you put a chatbot in a drone in a hospital or airport that would sort out the queries of visitors? Through facial recognition the drone would know who's in trouble and go to them and ask: May I help you?

11. Observe wildlife: If drones can be big and menacing, they can be small and inconspicuous and observe on the sly. They can take the shape of something that wouldn't alarm wildlife and act as a sort of candid camera in the forest.

12. Police the streets: Drones can act as a 24-hour police control and keep a lookout for suspicious activity and pass on the information to the control room. The police could also take charge of the drone and chase criminals.

13. Create mobile Wi-Fi zones: There have been many attempts to give Internet to the rural areas of India. Drones could move around as Wi-Fi hotspots from area to area. Facebook has been working on Internet drones powered by the sun.

14. Land surveys: Years back Karnataka did an ambitious Bhoomi project doing geographical mapping using satellite data. Imagine doing the same today with drones and a much detailed map of the land!

15. Advertising: Drones could be used for outdoor advertising. They could be used to carry banners, ads or even recordings to propagate a product.

16. Skyscraper maintenance: Drones could help in keeping track of what is going wrong in skyscrapers and maybe even do a bit of repairing and cleaning at the higher levels.

17. Carry people in emergencies: Drones are getting bigger and bigger and are able to carry more weight. The latest ones can carry people too. It could be used to evacuate people during emergencies or even some sort of passenger service.

18. Use in farming: In farming, a drone could be used to get detailed information in the case of large fields, spray pesticides and insecticides and even act as a scarecrow and chase away all the birds.

19. Site planning: Whether it is simplification at the pre-construction or things related to design drones can help in the planning of it all.

20. Asset management: Both governments and big companies can keep track of all kinds of assets with a fleet of drones.

21. Extraction pits for mining: This is also another hazardous area where drones can help out and save human lives.

22. Fish deep in a lake: This one is for fun. You could take the fishing line anywhere in the lake and fish wherever you wanted to. In this case, maybe the son could take his father fishing.

23. Replace the postal department: If the drones replace the delivery boy network, could they replace the postman too? Then the postal service would see a huge overhaul.

24. Take drone selfies: If you had a small drone of your own where you could attach your mobile, would you be able to resist the charm of taking selfies with it?

25. LED light show: We have had static light shows and musical fountains with light. You could put laser lights on drone or maybe even an army of drones to have a really wild light show.

WAITING FOR GODOT: 5 REASONS WHY 5G IS STILL HANGING

In the world of technology, nothing is more curious than the way in which 5G has been vilified, inadvertently stymied and virtually blocked in every step of the way since it was first discussed as a successor to 4G

Sunil Rajguru
sunilr@cybermedia.co.in

5G research started earnestly in the early 2010s and in 2014, Japan formed the 5G Mobile Forum.The International Telecommunication Union's IMT-2020 came the next year. In 2015 Huawei presented a testbed and the US freed frequencies the subsequent year. When dozens of countries completed 5G trials in 2017, one would have thought that 5G was just around the corner. However after that the implementation has been scattered at best.

So, is 5G really that good and worth pushing? IEEE Member Ramneek Kalrais very gung-ho, "There is no doubt that the way we work is changing. Remote work could become the 'new normal' especially with the approaching 5G revolution. With a lower latency, the biggest impact 5G revolution will have, is increasing the speed of cellular connections. A slow and unreliable Internet connection could become a thing of the past, and people in the future might not have to rely on Wi-Fi hotspots. Additionally, with the onset of 5G, employees will be able to get work done quickly and reliably, and hence, will be more productive from anywhere at any time. With the 5G revolution, the world will be better connected than ever before"

It's that simple as that for the common man. He needs more bandwidth on the go (as the mobile workforce mushrooms), for small businesses it could be a boon and now with the Work From Home Era taking off, 5G could well be a necessity for most

struggling in the lockdown.There wasn't that much controversy in the journey from 2G to 3G to 4G. They even managed to fit in 2.5G (GPRS) and 2.75 (EDGE) without much fuss, if you remember.

But the path from 4G to 5G was always different. Explains Amitabh Satyam, Chairman of Smart Transformations: "5G combines several new technologies with a newer set of frequencies. So, 3G to 4G upgrade was simpler as we used the same towers. 5G deployment is expected to start with deployment of new antennas closer together." Satyam was also Head of Operations of Reliance Communications in the early days.

It doesn't end there. Says Pravin S Bhandarkar, Founder and CEO of RtBricks, "Whenever 5G comes, what will change first is the radio. But the thing about networks is they are only as strong as their weakest link, and the much of the network will remain on a 4G back-end for some years. You will not have true user experience until you've done the whole upgrade."

It's not just the technology.There have been many other roadblocks…

1. The Indian telecom crisis: After the disruption of Reliance Jio, the Indian telecom industry has not been doing that well. The losses have been mounting as Vodafone struggles to stay alive and BSNL seems like a white elephant waiting to be rescued fully by the Indian government. Jio and AirTel are the market leaders, but the cash flow has been far from great. The entire industry doesn't seem ready to make the giant leap. To be frank, the way it has been, we would have struggled to even go from 3G to 4G with such balance sheets. That way the Jio-Facebook must be a lifesaver for the former, but how this affects 5G remains to be seen.

Continues Satyam from his earlier comments: "The rollout in India would be expensive and slow. Extensive trials are also required. Operators must develop business models to monetize 5G investments with the offer of higher level of security, lower latency, and the control on quality of services. Regulations must support such endeavours."

2. The Huawei Ban controversy: In 2015, Huawei had come out with first-ever "5G testbed" on the sub-6 GHz frequency band. China started whizzing ahead and other countries joined in like South Korea and Qatar. Huawei has been the world's number one telecom supplier and would have been essential in 5G implementation around the world but was hit by the ban from the US. The US-China trade war only made matters worse. India has also had issues with Huawei in the past even though the latter joined hands with Indian operators for trials. There have been a lot of controversies related to China and surveillance when it comes to 5G networks.

3. Health and interference concerns: Another issue was that of electromagnetic interference. There

were concerns that remote sensing and weather satellites would be affected. Then there have been persistent rumours of 5G being bad for health and the conspiracy theories around that are quite popular and widespread. There are small towns and cities all over the world that have banned 5G or planning to for this reason. That never happened with 3G or 4G! Adds Satyam: "These are in the realm of activism. There is no evidence of any health concerns due to higher frequencies of 5G."

4. Lack of leadership: Europe's CERN was at the forefront in the formation of the Internet and the UK was way ahead in a lot of research that took it forward. On most issues, Silicon Valley takes the clear leading role when it comes to implementing any technology. India became a major in IT services. But that has not been the case with 5G.While implementations have been there, no country has taken the bull by the horns and managed to inspire all other countries. Earlier it was China that was taking a clear leadership role. That was severely dented first by the Huawei controversy, then the trade war with the US and finally Covid-19.

5. The Covid-19 crisis: This brings us to the Corona Age, which has turned the world upside down. It spells bad news for 5G from each and every angle: The economy, China and the Indian telecom industry. Implementation will be even tougher now.5G will be more capital intensive and you will need smaller and more numerous towers placed closer together. In an era of no-touch, WFH and lockdowns, how are you going to get contractors and workers to implement it all across the country and with the desired speed?

There's another bizarre thing happening. 5G has actually being accused of creating the Covid-19 virus! It so happens that Wuhan was one of the first cities where 5G trials were held and that has led to a myriad of conspiracy theories which have been read and viewed (the conspiracy videos are elaborate) millions and millions of times. So 5G somehow created the virus or enhanced it, depending on which theory you read. It didn't endthere: People have actually gone around burning cell towers and destroying telecom equipment. There have been more than 100 such incidents in the UK alone. One newspaper reported that in one of their towns, when a woman saw workers laying optical fibre cables,she exclaimed: "When they turn this on, it's going to kill everyone!" As expected, most of the telcos simply refused to comment on this particular controversy.

What about 5G mobiles? That's another industry that can take off only if the networks are in place. It's a sort of chicken and egg situation. The lockdown could last for months and some sort of partial lockdown and the economic crisis could last for a few years. It is safe to say that the world may be focussing on essentials till maybe 2021-22 and anything related to 5G maybe not classified as an essential though one could argue that it is essential to the WFH culture that has been supersized off late.

Says Rajan S Mathew, Director-General of the Cellular Operators Association of India (COAI): "5G adoption and implementation in India, although ardently supported and encouraged by the government, faces many challenges. Among these are the high price for the spectrum, multiple claims on the limited spectrum being put up for auction, lack of use cases tailored for India, the lack of financial resources with incumbent operators to invest in new technology because of their deep financial distress, etc. There has now been added another woe—the Covid-19 pandemic. Globally, this has forced many countries to postpone planned 5G spectrum auctions and operators pulling back from planned investments and implementation. In India, the onset of Covid and all its attendant challenges has ensured 5G adoption will probably be now pushed back well into 2022 or even 2023."

Another important factor as a result of Covid is the no-touch technology and maybe the need for driverless and connected cars. Damien Stephens, Associate Vice President, Mobility & IoT, Tata Communications, told us much before this whole crisis started, "Customers can potentially get everything in their car, and automakers are planning for this already today. There is high throughput capability going into vehicles and combined with 5G, this will enable cognitive-speed response times that will help to bring about autonomous vehicles. And when we don't need to drive the vehicle anymore, we can sit and watch movies, or work, or read, or scroll through news feeds. This will impact all of us as consumers of course, but the impact on the automotive, telecoms, advertising and content/ streaming industries will be immense."

As you can see, 5G is crucial for a lot of things: Internet of Things (IoT) devices—wearable and industrial, Industry 4.0, better smart homes (connected buildings) and smart cities, logistics, shipping and fleet management… A lot of things will be left hanging. What is the solution? Can we simply leapfrog to 6G? Says Satyam: "6G is too far and we do not know what it stands for yet. So, 6G cannot be in the equation anywhere today."

After Covid-19 we are seeing a lot of technologies getting accelerated: Collaboration tools, drones, medical technology, Artificial Intelligence, OTT networks, cloud… Ideally 5G should have been on top that list, but that doesn't seem to be happening yet.

Much like Waiting for Godot, in technology, it's still Waiting for 5G!

MOVING FROM DIGITAL ERA TO DATA AGE

Factoring in the time, money and return on investment realized in moving backup and archive to the cloud—for virtually all business—the process of backup is now a strategic advantage

Sameer Bhatia

Data is the heart of digital transformation. Today, companies are leveraging data to improve customer experiences, open new markets, make employees and processes more productive, and create new sources of competitive advantage—working toward the future of tomorrow. In a report sponsored by Seagate, IDC found this digital transformation will generate data that will grow to 175 zettabytes by the year 2025. That's more than a tenfold increase from the 2016 levels of 16ZB. IDC calls the current era the Data Age, where everything we do is fundamentally changed by the advent of autonomous vehicles, humanoid robots, smart homes, and smart factories—and the data they bring into being.

Expansion of datasphere

Data is generated at three key locations where

content is actively created by individuals and organizations. First, the core (traditional and cloud datacenters), second is the edge (enterprise-hardened infrastructure like cell towers and branch offices), and third, the endpoints (PCs, smart phones, and IoT devices). This data created is propelling the tremendous global datasphere expansion and therefore, stemming the demand for data storage. IDC forecasts that over 22 ZB of storage capacity must ship across all media types from 2018 to 2025, to keep up the storage demands.

Data storage trends

Data storage has evolved to the next stage ever since Industry 4.0 revolution disrupted the way we use data. By 2021, there will be more data stored in the public cloud than in traditional datacenters as per IDC. Given the unpredictable data explosion from various sources, storage industry is looking at demands from both consumers as well as enterprises. The continued growth of applications and services means that the volume of media devices (hard disk drives, flash drives, SSD) for storage will grow. As software-defined everything (SDx) enables IT teams to scale up operations in the most cost effective way, more and more businesses move from client/server model to a mobile/cloud world. This means, we are looking at demand for mass capacity storage devices of up to 20TB being deployed in the cloud. For example, simple tasks like expense tracking for business travel used to be tracked in spreadsheets. Now they're handled with a mobile app that captures pictures of receipts; that data lives in the cloud.

Backup to stay secure

As businesses are migrating to digital transformation and deploying new-age technologies such as AI powered applications and cloud services for their customers at a rapid pace, the data protection, storage and recovery landscape is undergoing a paradigm shift. Due to this shift, large amount of data is being generated. It is a perfect time to start thinking about how to protect all your data. In the past few months, backing up to store data has gained supreme importance as globally information is being exchanged online and there is more data in circulation than we ever imagined before. The accelerated digitalization, driven by unprecedented circumstances, has made organizations and individuals to save data securely and maintain proper backup to enable recovery in case of an unforeseen technology disaster.

SAMEER BHATIA, Country Manager for SAARC & India, Seagate Technology

On March 31st every year, we acknowledge World Backup Day to emphasize the significance of preserving data and according to the organizers of World Backup Day—almost 30 percent of us have never backed up our data! Because we carry our devices (the endpoints of data creation) with us almost everywhere and all the time, the chances of losing valuable information are higher. Two basic tips that can help everyone to back up their data effectivelywould be:

Be Prepared—Being aware of potential vulnerabilities and staying prepared is the key to recovery from any disaster that might happen when it comes to your critical data. Plan and schedule back up regularly from devices as well social networks. Businesses have a pre-scheduled data backup system to ensure storage on cloud, data centres for faster recovery.

Be Organized—It is a great way to store, use and manage data across devices and networks. Cleaning up irrelevant content, freeing up space, maintaining data by regularly backing up helps save the panic when an uncertainty hits. Organizing content in files, folders and drives keeps the data securely stored for a longer time.

Choose the right drive

Once, the preparation and data organization is done, the next step is to understand the storage need and choose a device that fits. Here are some tips that may help in choosing the right drive:

Easy access—In case you are a movie fanatic, music lover, photographeror a blogger and you prefer carrying your content with you, storing on a portable drive could be a great option. The accessibility it offers on-the-go, anytime is what makes a portable drive suitable for backing up such data. However, knowing which content is needed all the time is integral to segregate and store old assets on the cloud or a backup drive and make room for the data assets you need daily.

Think capacity—Take stock of your data. Whether you data is just small files and folders or multimedia content which needs more storage space will be the differentiator for your storage requirement in choosing the right drive. If you've got a smaller amount to store, a mobile drive with 1-2TB of storage would likely be sufficient but if you have tons of media assets, then a higher capacity drive with up to 8TB storage or 10TB hub may be a better fit.

In case of enterprises, modular storage systems and solutions that are engineered to help you efficiently move data around your enterprise, cloud and edge are suitable. Such products offer a variety of storage options and configurations that are simple, secure, and efficient for emerging datasphere environments.

Factoring in the time, money and return on investment realized in moving backup and archive to the cloud—for virtually all business—the process of backup is now a strategic advantage.Because backup has everything to do with it there has never been a better time to move your backup data to the cloud.

Protect Your Data

How do we protect company data from the risk of security vulnerabilities? Remote working dynamicspresent an opportunistic circumstance for hacking and phishing attacks. To prevent businesses from losing control over data, protect your data with encrypted drive, look for Common Criteria accreditation for security features, and ensure every drive complies with the top industry standards for security—for instance, one that delivers protection that suits most needs, and one that meets requirements for government or enterprise customers running highly secure, data sensitive services and application.

In case of enterprises, modular storage systems and solutions that are engineered to help you efficiently move data around your enterprise, cloud and edge are suitable. Such products offer a variety of storage options and configurations that are simple, secure, and efficient for emerging datasphere environments

Awareness about the data preservation is important to protect the data. Today, there are millions of smartphones users and lot of content is being created with use of smartphones. According to the organizers of World Backup Day, almost 30 per cent of users never backup their data which increases the chances of losing the data more. A simple accident could destroy most important files as our devices are on the move most of the time. To protect data in all the right ways, a well-organized content with regularly planned backups helps in storing the data on computer, phone and other devices. The advantages of recurring backup's help in keeping the data secure round the year and provideeasy access to the information. Additionally, it is important to know the capacity of data to be secured one should choose the right storage drives to save the data.

Together with company-wide planning and employee education, enterprises are able to achieve seamless data management and support their employees.

The author is Director of Asia Pacific Consumer Business Group and Country Manager for SAARC & India, Seagate Technology

INDIAN SMART ECOSYSTEMS WILL DRIVE GLOBAL EFFICIENCIES

In addition to a global supply chain, global OEMs explore manufacturing opportunities in India considering the cost-effective nature of the country. Indian manufacturers are able to deliver high quality products with uncompromised global quality

Rajeev Kaul

India is at the cusp of a digitally connected future. Organizations must realign their strategy and business goals to remain agile to such change. Disruptive technologies will be at the centre of this new transformation and organizations will be able to leverage these technologies to improve their productivity, efficiency and quality.

The industrial automation market in India is worth US$2billion but the degree of automation depends on the organization. Major manufacturers in the industry are shifting to an automated line or shop floor by phasing out older equipment and upskilling the workforce. They have also deployed Internet of Things (IoT) in various stages to track processes and minimize redundancies. Other technologies such as Flexible Manufacturing System, AI, 3D printing, AR/VR solutions and robotics have also witnessed significant growth in India's shop floors. Such adoptions help to improve quality of production, reduce lead time, manage dynamic changes in requirements and equip a workforce with digital skills.

Creating smart ecosystems

According to a study by Deloitte Manufacturer's Alliance for Productivity and Innovation (MAPI), manufacturers who have invested in smart factories believe that they have been receiving a return on their investment through increased productivity and profit gains. The report further highlights that these manufacturers have seen over 12% increase in labour productivity, 11% increase in factory capacity utilization and 10% increase in total production output.

Smart factories are an amalgamation of these disruptive technologies that connect the physical and digital worlds of a manufacturing company. In order to do this, manufacturers must adopt a smart ecosystem that enables the convergence of Information Technology (IT) and Operation Technology (OT), vertical integration of manufacturing systems and end-to-end connectivity across the value chain. Smart factories take automation to the next step and give organizations an edge in their respective industries by creating efficient, agile and flexible processes.

Fulfilling customer expectations through smart ecosystem

With the changing global marketplace, customers now demand world-class products with aggressive deadlines. A smart factory will be well equipped to meet

changing customer needs. These ecosystems have already witnessed accelerated levels of productivity. This means, manufacturing processes can now keep up with such short lead times.

Besides this, integration of other technologies such as manufacturing automation, robotics and sensors, reduces human intervention and subsequently the chances of human error. They also monitor processes in real time to possibly prevent downtime or detect any other red flags such as potential equipment failure.

Future of digitization in aerospace manufacturing

With air traffic growing year-on-year, there is an increasing demand for aircrafts in the country. Aerospace manufacturing companies must combat this demand while ensuring zero errors, leveraging the benefits of digitalization and a smart manufacturing ecosystem.

Several leading aerospace manufacturers have shifted their focus to digitalization to make a key priority for their business. A strong digitalized approach will help create an ecosystem of innovation within the organization.

Technologies such as big data and sensor-based data analysis like automated dashboards are currently redefining the industry. Along with a Flexible Manufacturing System, AI and Machine learning, this creates an intelligent ecosystem that is adaptable to changes and has predictive maintenance capabilities.

Leveraging global competencies

Today's supply chain spans across geographies and leverages global competencies to provide the best results to customers. By definition, a global supply chain is large and has multitude of vendors, distribution centers, suppliers and manufacturing facilities among others.

A manufacturing company's digital transformation will also have a positive impact on its supply chain. With an integrated approach, leading Industry 4.0 technologies can be used to improve productivity and streamline traditional processes to minimize redundancies.

M&A—knowledge transfer

Companies must equip their supply chain with the right technologies that can help them fulfill changing requirements. They need to meet aggressive deadlines without any compromise on the quality. Predictive analysis can help manufacturers by forecasting expected demand, upcoming market trends and also identify potential points in the supply chain that could be inefficient.

Considering that a global supply chain will have multiple points of intersections, digital tracking enables to monitor the status of the manufactured part on a real time basis. This will further help companies update their

RAJEEV KAUL, MD & CEO, Aequs Aerospace

customers and identify any bottlenecks in the supply chain. Mergers and acquisitions with leading OEMs can further help improve global competencies by driving international standards of technology and knowledge transfer.

Making in India

In addition to a global supply chain, global OEMs explore manufacturing opportunities in India considering the cost-effective nature of the country. Indian manufacturers are able to deliver high quality products with uncompromised global quality. They provide significant savings throughout all the processes.

Manufacturing is set to drive India's GDP in this new decade. The Indian government has extensively provided opportunities through initiatives such as 'Make in India' and 'Digital India' emphasizing on the need to digitalize manufacturing processes. Digital elements such as flexible manufacturing, robotics and 3D printing have now found its way into the shop floors of India's manufacturing companies and have managed to create efficient smart ecosystems. Additionally, organizations need to reskill or upskilling existing employees and nurturing new talent in order to adopt relevant technologies rapidly.

Preparing for the future

Reliability is integral in every manufacturing process. Customers rely on OEMs to manufacture parts based on their requirements and OEMs depend on their suppliers and partners' support, in this process.

Such technology forward ecosystems and reliable supply chain will enable the Indian aerospace manufacturing sector successfully deliver parts to global OEMs as per the agreed competitive time. This will create the roadmap to India becoming a preferred destination for global aerospace manufacturing.

The author is MD & CEO, Aequs Aerospace

A STITCH IN TIME SAVES NINE... T-SHIRTS. MAY BE MORE!

HR Tech with AI can do more than clearing away HR's calendar and bandwidth for more important tasks. Siva Kumar, CTO, Zaggle tells us how humans are still, and in fact, more relevant with the explosion of AI in HR functions

Pratima H

What made you foray into HR and payment areas with AI?

This question can be answered with an interesting anecdote—an employee of an MNC approached his HR Head with 35 T-shirts in his hand from events that took place over two odd years. He explained how those T-shirts were a waste for him because he wouldn't wear them. That's when the company realised, they needed digital rewards for their employees to enable them to benefit from rewards.

Zaggle was born to fulfil this growing need for digital rewards. We first came up with employee benefits, then with employee reimbursements and then forayed into expense management. We are a payments company working in the areas of Financial Tech, HR Tech and Bank Tech and the most amazing part of HR Tech is that it deals with People and mapping AI to HR. We found our sweet spot in work force performance management, the modelling we did using predictive analysis (AI) as to what could be the career growth of an individual after he joins the company. This modelling is being appreciated by a lot of our beta clients and we hope to release it soon.

Can AI soon turn into a hygiene factor for the industry? Any way in which it can also shape into a strong revenue area?

If we see how the world has evolved around data in the last 20 years, you would notice that, earlier, the problem was the quality and quantity of data. Anybody who made data- driven decisions would say I don't have real-time data on hand. It was all based on historical data. Now that we have truckloads of real-time data, the skill required is (A) 'What to look at vs. What not to look at' and (B) How would you use that data. And that's how companies with the exact same data set end up making completely diametrical decisions.

The game has changed around raw data to data intelligence and data analytics and what you do with that data. Payments—that is of course a very important aspect and the data we have will help us develop solutions for our users. If you are not thinking AI into your products, you would soon be out of

business. So, it's already becoming hygiene. AI has already replaced the lower-end mundane jobs and is increasingly becoming a revenue generator or a cost saver. What we feel is that as we keep advancing in the product life cycle, AI will, possibly, become a major source of revenue rather than the cost cutter that it is majorly used as today.

It will replace the humans at the lower-end with the bots, but if you look at where the world has reached in terms of Sophia, the humanoid, I am pretty sure that we will be able to do most of the back-end analysis and analytics job with AI in the near future and sell the same as services to the other companies. It may, or may not, give direct revenue, but as we solve customer problems and simplify their lives by using AI, it would be adopted and loved by our customers and, hence, would indirectly give us growth.

Tell us something about how AI helps in expense management and reward functions? Do Propel and Save products use Deep Tech?

Yes, we do use deep-tech for both Zaggle Propel and Zaggle Save, which are integrated platforms for workforce reward and recognition, employee engagement, and state-of-the-art AI-powered performance management. AI is deep into our products and is present everywhere.

Can you explain with any examples?

Today, as part of the accounting process, you would have to submit the invoices to support the expenses that employees incur during their day-to-day operations. Imagine as an employee, I would need to read the bill, enter merchant name, date/time, amount spent including tax break ups etc which is pretty labour-intensive. But we have almost done away with that laborious process. The moment a bill is uploaded on Save, we convert the bills uploaded as images in to text by using various AI techniques like OCR, entity extraction, NLP etc. So, in real time all the information is converted to text. On top of that, if the accuracy of the automation goes beyond a threshold figure configured by employers, we disable editing of the expense by employee. So, as a manager who is approving this expense need not figure out if the merchant name really reflects what employee is claiming, whether the date and time the expense happened and the amount claimed all are matching with the bills. It is a such a joy experienced by both employees and managers.

For the rewards and recognitions management

SIVA KUMAR, CTO, Zaggle

program, we offer rewards cards for employees and we have also tied up with more than 8500 merchants such as Abbot, Vodafone, Samsung and many more.

How crucial are moves like Open Banking, CMA guidelines and industry consortiums for the industry?

Open Banking is a beautiful concept and has been around for more than a decade around the world, but it hasn't taken off yet especially in India because it requires the necessary surrounding-infrastructure for it to function. But with the advent of UPI stack, it took off suddenly and now the number of use-cases being built around it is huge. With standardisations by means of guidelines and consortiums, it would become far easier for FinTech players to not worry about the bolts and nuts of how to build but they can rather focus on what to build.

Another important reason is to draft uniform regulations or codes of conduct that will govern individual companies throughout that industry, and to set standards for the licensing of professionals within an industry.

Is the impact of new APIs going to be strong for new revenue streams?

Application Program Interfaces (APIs) are basically interfaces which the third party can use to build a service of its own. We do assertively believe that the impact of these new APIs will be much stronger for

the new revenue streams.

The new APIs make it easier for different technology platforms applications to interact with each other in a commonly-understood language. Furthermore, APIs offer companies the opportunity to increase the revenue, ease down the integration of backend data applications, adopt innovative solutions, reach a wider audience, and effectively support their sales and marketing activities.

AI's success depends on data—would players, including archrivals, come together to expand the scale and depth of AI data?

I believe that AI is still at its nascent stage in India. As a thumb rule, I strongly believe in Andrew Ng's philosophy that we can only do those things with AI that a human can do in a second or less. To point an example; in HR, we can probably automate if an employee is happy, anxious, worried by taking a picture of an employee and feed into AI and it would pretty accurately be able to predict the emotional state. But, AI at its current state of development, is not good enough to go beyond that. For example, based on the emotional state, an HR manager can have deep conversations understanding the situation that employees go through which would take minutes or even hours to figure out the issue with the employee and then come up with empathetic suggestions. Here, AI is not even close though there is extensive research going on to match human capabilities.

Any challenges that AI faces when it comes to matching the quint essentially-human factors in HR functions?

One of the major challenges is that using AI while recruiting lacks the human touch in the entire hiring process. Another one is that reliability may still emerge as a question and prove to be a matter of concern. Since the data-learning process may still have numerous inconsistencies and flaws in it, reliability stays as a major issue.

What shifts, if any, are happening to embrace the impact of new concepts like Blockchain, AI, BaaS (Banking as a Service), Digital-only banking, FinTech-based financial inclusion?

We see a world where every company is embracing new FinTech products that offer all banking services and tons of additional features that banks cannot and should not imagine. With banking data and services opening up, FinTech players would come with so many innovative and disruptive ideas by combining AI/Blockchain along with massive banking data that we cannot imagine any business or even individuals going to physical banks anymore in future.

That new innovations are set to have such a major impact on retail banking in the next few years; and this shift suggests that regulators have come to a point where they can allow these technologies to flourish. With more governments, regulators and even businesses embracing these new concepts, it seems certain that it's only a matter of time before AI-based business on a mainstream level becomes a norm.

Can AI help evade bias and abuse—especially in HR?

We humans make sense of the world by looking for patterns, filtering them through what we think we already know, and making decisions accordingly. When we talk about handing decisions off to AI, we expect it to do the same, only better. Harmful human bias, both intentional and unconscious, can be avoided with the help of AI, but only if we teach it to play fair, and to constantly question the results.

Humans are hindered by both their unconscious assumptions and their simple inability to process huge amounts of information. AI, on the other hand, can be taught to filter irrelevancies out of the decision-making process, pluck the most suitable candidates from a haystack of résumés, and guide us based on what it calculates to be objectively best rather than simply based on what we've done in the past.

In other words, AI has the potential to help us avoid bias in hiring, operations, customer service, and the broader business and social communities—and doing so makes good business sense.

Is that where humans become more relevant?

Humans must tell AI what they consider suitable, teach it which information is relevant, and indicate that the outcomes they consider best—ethically, legally, and, of course, financially—are those that are free from bias, conscious or otherwise. That's the only way AI can help us create systems that are fair, more productive, and ultimately better for both business and the broader society.

Today, AI excels at making biased-data obvious, but that isn't the same as eliminating it. It is up to human beings to pay attention to the existence of bias and enlist AI to help avoid it. That goes beyond simply implementing AI to insisting that it meets benchmarks for positive impact.

Yes!
I want to subscribe to PCQuest

	Period	Issues	Price for New Subs.	Price for Renewal	Your Benefit Zone
☐	1 year	12	Rs. 1500	Rs. 1350	Save 10% on renewals
☐	2 years	24	Rs. 3000	Rs. 2700	Save 10% on renewals
☐	3 years	36	Rs. 4500	Rs. 4050	Save 10% on renewals

Please tick your subscription choice above, fill the form below in CAPITAL LETTERS and mail/fax it to us.

☐ 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 can be faxed to:

0124-2380694 or mail the form with payment (cheque/DD) to:

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

Terms & Conditions:

• This special offer is valid for a limited period. • 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 delivery 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 disputes shall be subjected to Delhi jurisdiction only.

HOW AI-ML & DATA SCIENCE CREATE A PLATFORM FOR ADAPTIVE LEARNING ONLINE

Online learning has taken a lot of tedious procedures such off the back of the teachers. A significant portion of work is automized, creating more space for a teacher to focus on designing learning modules. AI-ML can easily identify correct answers and catch plagiarism, if any

Randhir Kumar

The ongoing global pandemic, followed by the worldwide lockdown situation,has opened up unexpected avenuesfor pioneering educational reforms in the shape of Edtech startups. In these unprecedented times, when all educational ventures are in a limbo, online learning has come to conciliate dulled hopes of students.Online learning is the kind of learning that incorporates top-end tools such as Artificial Intelligence, Machine Learning, and data scienceto buttress textbook learning.

In today's time, the saying "one size fits all" has become archaic. Because of diversified needs, attention spans, and behavior, every student requires a unique educational model to grasp the concepts of a particular subject. The potpourri of the technological tools that are used on an e-learning platform establish such an environment for learning, where the caliber of each student is analyzed to concoct personalized modules that ensure and enable them to engage with the subject in the most efficient and effective fashion. Let's take a closer look at how the new technology is transforming the educational game altogether.

AI is already revolutionizing major industry verticals, the education industry is no stranger to its advantages. In the e-Learning space, AI is harnessed to systemize all student-related data such as current

grade, subjects, previous scores, competence, interests, and academic goals, and creates a database for each student. By sifting the learning dynamics of each student, AI enables an e-learning platform to provide a student with a holistic and adaptive learning module where s/he can make progress according to their own pace.

All this congregated information is too enormous for a single teacher to handle, this is where data science is channeled to arouse meaning from big data. The recurring patterns are deciphered by measuring the pace of a student, their comprehension, and application of the knowledge are diagnosed through tests to understand the level of competency in different subjects. Subsequently, an individualistic learning module is formulated and recommended to the student.

Once the learning journey begins, a predictive feedback framework is established through Machine Learning. The more information the computer feeds, the smarter it becomes at analyzing the trends of a student. Such data is congregated in creating a report which sheds light on the strengths, weaknesses of the student, so that the teacher can align their approach to match the pace of the student for a personalized learning experience. It doesn't stop there, additional supplementary lessons, courses are recommended to the student so that they can grasp the concept in its entirety.

Such technology also enables a more globalized learning experience. Students from different nations, irrespective of their native tongues, can come together on a single platform, and learn a subject of their choice. There are many extensions that can be used to provide live-captions for videos in different languages. Moreover, there's potential to even hold online student exchange programs or collaborative projects between students from different countries.

But online learning is not just limited to learning. With the help of AR and VR (Augmented Reality and Virtual Reality), online learning platforms are creating simulation games that put a student in a life-like situation to test the application of knowledge. Gamification is a new trend that's being witnessed in the online industry to further engage their students in their online community. Students are being encouraged to compete against fellow users on the platform on discussion forums, in quizzes and games to gain/earn points or collect badges and improve social standing on the platforms.

Similarly, the online learning method has also taken a lot of tedious procedures such as taking attendance, grading assignments and test papers, forming test papers, etc off the back of the teachers. With the help of AI and ML, a significant portion of work is automized, creating more space for a teacher to focus on designing learning modules for students. In the case of grading papers and submissions, AI and ML can easily identify correct answers from its repository of information and catch plagiarism, if any. In this manner, the chance of biased grading is also eliminated, as the papers are being scrutinized by machinery and not humans.

RANDHIR KUMAR, Founder and Chief Mentor, BasicFirst Learning OPC Pvt. Ltd

AI and ML are also used on e-Learning platforms as a virtual assistant to lend support to students, teachers, and parents alike. Be it queries related to academics, admissions, technical, or others, AI and ML, in the form of chatbots interact with people to offer answers to questions through a feed, or sort the queries by referring them to the person in charge. Similarly, through subscription-based feed framework, the online platforms offer daily updates to its online community. The content is specialized for students, parents, teachers, and alumni to keep them up-to-date with the latest developments on the platform, in the industry, and their preferred sector of the profession.

Needless to say that today, technology truly has transformed how we used to perceive learning. Going by the records, the world will surely see many more digital revolutions in the future to come that will create ripples in the industry.

The writer is Founder and Chief Mentor, BasicFirst Learning OPC Pvt. Ltd

GAMING INDUSTRY: THE IMPACT OF COVID-19 PANDEMIC

Ashok Pandey
ashokpa@cybermedia.co.in

Our lives have been changed in the past few weeks, most of us are quarantining due to COVID-19 pandemic. This lockdown is impacting billions of lives and industries. As we are spending our days at home, thus the consumption of internet and games has increased a lot.

People across the globe are looking for a way to distract and entertain themselves, a favourable time for mobile apps and games. Spending on digital video games hit a record high US$10bil in March as per SuperData report on April 23.

Spending climbed 15 per cent on mobile games, reaching US$5.7bil in March, SuperData reported. The mobile gaming industry has witnessed a huge surge, though it is for a short period of time. But there always two sides of a coin, on one side we have seen huge growth on the other side, many events and products either cancelled or delayed.

Cancelled Industry events

Entertainment Software Association cancelled this year's E3 event which has been the go-to annual occurrence for the video game industry since the '90s.

All competitive live events for **Electronic Arts'** games are suspended including EA runs.

Activision Blizzard Esports decide to cancel all Overwatch League events in both March and April.

EVE Online's Fanfest annual event has been cancelled due to COVID-19.

Activision Blizzard decided to cancel **Call of Duty League events**, moving all matches to an online-only format for the remainder of 2020.

GDC (Game Developers Conference) is postponed to avoid the virus' spread.

The **Taipei Game Show** was postponed until June 25–28, 2020.

The **Mobile World Congress** was cancelled as several of the China-based vendors had to cancel plans.

PAX East was cancelled as vendors withdrew or scaled the plans back to present their products.

The 16th **British Academy Games Awards** are moved to a live-streamed event due to concerns over the coronavirus.

The physical 2020 **Gamescom event** was forced to cancel as Germany banned public events.

ESL Pro League Season 11 Global Offensive

tournament, ESL announced that both the regular season and the finals will be split into two regions: Europe and North America and that regular season and the finals will be played entirely online.

The ongoing series of the 2020 **Pokémon World Championships** was cancelled by The Pokémon Company.

The League of Legends Championship Series and the League of Legends European Championship were suspended on March 13 and resumed play as an online-based format on March 20.

The live **Rocket League World Championship** for its 9th season, planned for April 24, 2020, in Dallas was indefinitely postponed.

The **Overwatch League** cancelled those occurring in China and moved them to later in the season to South Korea.

Production delay

Nintendo Switch – The production is delayed for the Japanese market, leading to shortages of Switch consoles, accessories, and games.

Oculus Quest back-ordered – The Quest is out of stock on the company's website, Best Buy, and Amazon.

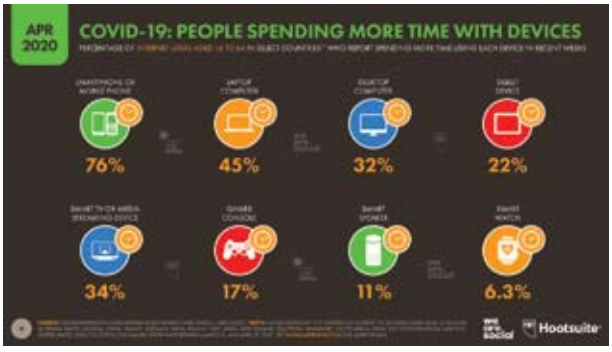
Outer Worlds port for Switch delayed – Virtuous, the Singapore-based studio, is working on the port, but Private Division game is not going to be available soon.

TurboGrafx-16 Mini delayed – The plug-and-play console is delayed indefinitely because of the coronavirus.

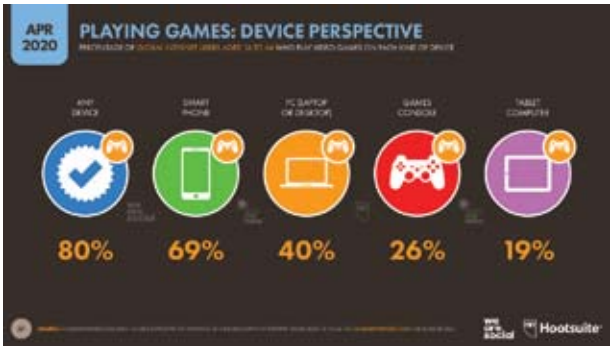
Valve Index – Valve Index virtual reality headset production was reduced due to the impact of the coronavirus.

When events and productions of the game being cancelled, the mobile gaming world has seen a huge growth in downloads. GlobalWebIndex reveals that people all over the world have been spending considerably more time on their digital devices as a result of coronavirus lockdowns.

76 per cent of internet users are spending more time using their smartphones in recent weeks compared to their pre-lockdown behaviours.



If most of the users are spending on their smartphones, then what are they doing? Well, games are their top choice, the data from App Annie shows that weekly downloads of mobile games in March 2020 jumped by 30% compared to weekly averages for the final quarter of 2019. In total, over 13 billion games have been downloaded during the first three months of 2020. And 69 per cent of the users are playing games on their smartphone.



Conclusion

A majority of countries are under lockdown and a global recession looming. Though we have seen a huge growth in the online activities still it is too early to measure the impact of the pandemic on the gaming industry. But, looking at the steady rise in the consumption of online gaming will witness a good amount of investments.

OF MOBILE VANS AND MOBILE APP PAYMENTS

Rohit Kumar, CEO & CMD, XPay.Life talks about how they help with bill payments in rural and Tier-2/3 cities via ATP kiosks, PoS machines and mobile vans at the same time providing earning opportunities to franchisees as well

Sunil Rajguru
sunilr@cybermedia.co.in

How does the whole thing work? The process of payments for B2B and B2C?

The B2B and B2C processes are quite different from each other. For individual customers, the ease of usage is important. The process of utility bill payment for the customers is facilitated by digital solutions such as mobile applications and the website. We cater to the B2B sector by offering ATP kiosks, PoS machines and mobile vans to the billers and providing earning opportunities to the franchisees as well. These will facilitate bill payment to the customers who reside in the Tier2 and Tier3 cities as well as the rural areas of the country.

What are the benefits for merchants and for consumers?

Customers can benefit from the seamless process of immediate and secure payment of their utility bills from the mobile app and online Web. The platform also enables them to use cash as a form of digital payment along with other digital payment methods such as UPI, credit/debit cards, Internet banking, mobile banking and using UPI payments. There are zero convenience fees/Internet charges for below and above Rs 2000, hence customers need not pay a single penny extra on their bill.

They can also avail the banking facilities that the mobile van provides along with facilitating bill payment. This is a boon to a customer who resides in the most remote area of the country and would need to travel more than 40–50 km at the cost of his daily wage either to pay utility bills or to access an ATM. The merchants can own a PoS machine and the mobile van on ownership or franchisee models and

earn extra income without any potential risks.

Is this focused entirely on semi-urban or rural markets? If yes, why?

As per a google BCG report, 80% of the rural population and 20% of the urban quanta still depends on cash payment for all their day-to-day financial transactions. XPay Life caters to both the rural and urban sectors by providing infrastructures like ATP kiosks, PoS machines and mobile vans that accept cash as a digital payment method.

What are the advantages over (or comparison with) existing digital payment systems like Paytm (which reportedly also works with US$)?

Our mobile app is built using one of the most secure payment technologies of blockchain which is the underlying technology for cryptocurrencies like bitcoins. So, the payment gateway is highly secure. We are a BBPS/NPCI approved agent institution and all the payments are BBPS assured. One other safety measure we have incorporated is that the XPay.Life doesn't store any credit/debit card details and hence safeguarding the customer confidential data like card details, CVV number, etc from the prying eyes of the cyber fraudulent.

The government has been looking to drive the transition of the country from a cash dependent one to a cashless economy. Similarly, we too, want the transition to happen from the traditional cash dependency to the digital modes which are quite a cumbersome process in the semi-urban and rural areas. Hence we are easing the process of this transition, making it simplified for the users.

Who are your current customers? What are the types of businesses and consumers using your existing services?

We currently have a pan India reach with customers from across the country. From individuals who use it for everyday bill payments to businesses who look at more large scale transactions, we have a wide customer base. Customer base in 200+ cities and for B2B almost all the ESCOM's are using our services. As of now we have 10 lakh+ customer pan India.

Who is your target audience for the future? Primarily cash users?

Our target audience is a mix of tech-savvy mobile app users and also the cash users who prefer paying through queues at the biller's collection points

ROHIT KUMAR, CEO & CMD, XPay.Life

and the customers from the rural region who are intimidated by the complex online payment modes. Being an economy that relies largely on cash, it is not easy to make the shift to a cashless economy overnight. We are providing infrastructure that makes it simple to pay by even using cash as a digital payment mode and will help rural India to educate/ train them to become digital subsequently .

Apart from security enabled by technology such as AI and Blockchain, what are the advantages that the new product provides over existing solutions?

XPay.Life is built on the most stringent business model of AMBIC that stands for Artificial Intelligence, Mobility, Blockchain, IoT, and Cloud. We are leveraging futuristic cutting edge technologies for the platform. India has a significant percentage of non-English speakers. To make it more user-friendly, we have made the app and online website available in 13 regional languages. Also, the login procedure is simplified so that account authentication can be done by providing the phone number or directly logging in through Facebook or Gmail. We are easing the bill payment process in the semi-urban and rural sectors by accepting cash as a digital payment mode along with other popular digital modes of payment.

The mobile van facilitates banking and bill payment to the most remote villages by traversing the strategic, pre-defined route and is owned by the billers of that region thus making bill collection easy through the ATP kiosks and facilitating banking facilities like cash-withdrawal through the XPay.Life mobile van. We are the first in India to build a digital solution to onboard a majority of rural India on to the digital bandwagon.

RISING PENETRATION OF ONLINE GAMING IN TIER 2/3 TOWNS

Various online websites, institutions and e-learning platforms providing training to millennials to master skill-based games

Rai Sahib Singh Khurana

In today's advanced Uber-connected era, technology leeway plays a significant role in the development of a nation. Everything is reliant on modern-day technology because it has improved our lives, made it more accessible and engaging. The rapid adoption of smartphones and the availability of Internet facilities is providing a whole new realm of opportunities for unconventional industries like the gaming sector as well. It would not be wrong to say that the advent of the digital age has revolutionized the gaming sector.

Innovative technologies ensure to boost entertainment values by providing immersive experiences to the players. However, digitalization has not entirely engrossed in some unexplored rural sector due to intense disparities brought by social, financial, geographic and many other factors. Therefore, due to the extensive Internet penetration, Tier 2/3 towns in India are slowly becoming digitized and accessible to new forms of informative tools. Digitization is a huge game-changer that is offering infinite opportunities to all gaming companies in the business, irrespective of how big or small they are.

The current scenario in the Indian gaming industry

As the gaming industry is evolving continuously with the advent of modern technologies in India, a massive transformation is due to the emergence of smartphones. They offer high-end technology at affordable prices.

As a result, gaming is one such entertainment option which is enjoyed by everyone. More engagement over gaming platforms has resulted in redefining the dimensions of the gaming industry. The advancement in gaming technologies over the years has resulted in the generation of larger revenues. According to Statista, the gaming industry was expected to generate revenue up to INR 120 billion by the financial year 2023, indicating a significant growth potential in the industry. The fast-

paced growth in online gaming is due to an increase in digital population with access to speedy and cheap Internet.

Overall, Indian gamers prefer more mobile games than PC or console games, mobile games users across the country are projected to reach about 370 million users by the year 2022. Showing a significant boost in the number of users due to the availability of high-speed Internet, developed tools and apps (Apple app store or Google Play). Skill-based games and fantasy games have witnessed the highest growth in India. With the help of the newest technology, our favourite card games have now become hassle-free and more enjoyable. Skill-based games like Poker, Rummy and Fantasy Sports have become the latest rage among online players.

Technological advancement has influenced skill-Based gaming in India

Today's gaming world has upgraded in comparison to what it was in the last couple of decades. Upgraded technologies are evolving at an impressive rate which has resulted in mobile apps offering unrealistic and unmatchable gaming experience. The new and innovative technology has exhibited innovative features and new formats in skill-based games which attract more players towards the game. The gaming apps ensure that their user data, transaction details and personal information of their players remain safe as they enjoy gaming worry-free. Skill-based games like Poker have been remodelled and easily available on online websites or mobile apps in a more interesting and thrilling form.

India has always been a hub of skill-based games, board games like Chess or Ludo and card games like Teen Patti, Poker or Rummy. Indians used to play these games way before any computer or console games. The population is now graduating towards skill-based games due to cheap internet facilities, and availability of smartphones at cheaper rates. The introduction of gaming apps in smartphones like Teen Patti Gold - 3 Patti, Rummy, Poker Card Game, Chess app, etc. has promoted the growth of skill gaming. There are other game-changing technologies which are transforming skill-based gaming in India like Big Data, Cloud Computing and Advanced Cloud Services, Gamification, Mobile gaming, Augmented Reality, VRConsoles, Blockchain.

New- Age technology exposure to Tier 2/3 towns

Penetration of skill-based gaming in rural areas, especially in Tier 2/3 towns, has been comparatively

RAI SAHIB SINGH KHURANA, Founder, The Big Stack

slower than their urban counterparts, majorly due to lack of awareness regarding the use of digital technology. Many gaming companies are realizing the market potential in vernacular sections of India and are making desperate attempts to reap the benefits of huge opportunities hidden in Tier 2/3 towns to target their audience there.

Various advanced skill-based learning systems that are self-diagnostic, game-like, and competitive, engaging mainly focused on giving the users an immersive experience. Various online websites, institutions, e-learning platforms providing training to millennials to learn the game as well as master skill-based games. They help in making the entire gaming and learning experience fun-filled by evaluating skills through quizzing, interactive sessions, providing ample opportunity to resolve queries using webinars. Due to technology, these skill-based learning systems are easily accessible for users anytime and anywhere, especially living in rural areas and Tier 2/3 towns.

Future of skill-based gaming in India

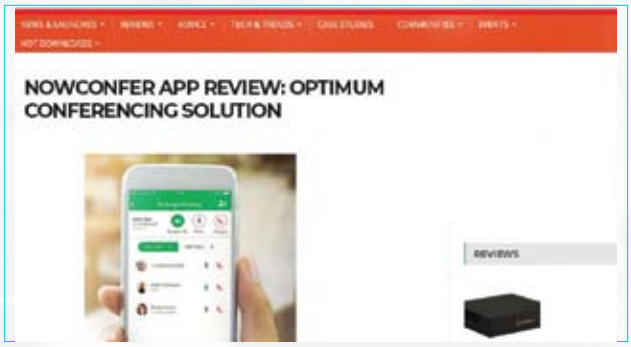
The gaming industry is growing at an exponential rate. The line between real and virtual life is getting blurred with new technology each passing day. The future of skill-based games will be more interesting as the reports indicate that the value of the gaming industry in India will be worth over INR 250 billion by 2024. The rage for real money or skill-based games is driving a lot of variations in the gaming industry focused on improving the user experience. In the future, technologies like AI, VR, and Augmented Reality will be incorporated in skill-based games to make sure users get more immersive gaming experience.

The author is Founder and CEO, The Big Stack

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

SOFTWARE

HOUSEPARTY REVIEW

— Ashok Pandey
ashokpa@cybermedia.co.in

Houseparty, the name itself defines its purpose, enabling us to connect with the people we care the most. The social networking app has gained huge popularity in the past few days. It is dominating the download chart on both Google Play and the Apple App Store.

The face-to-face social networking app, not only connects you with your loved ones but let's you chat and play games with your friends and family.

The experience

Houseparty has gained a lot of popularity in the past few days. It has intuitive UI with one aim to offer its users a quick group chat (Party). At first sight, it looks interesting, when you start using the app, some of the features look similar to WhatsApp and Snapchat, but not exactly with improvements. It is a good mix of both apps.

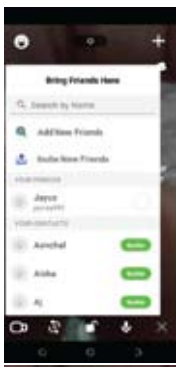
Using Houseparty, 8 people can join in a video chat at one time. When you or your friend, connect over a Houseparty, others get a notification to join the chatroom. The trouble is your friends can start the party anytime, and if you are connected with multiple groups, then you should be ready to get plenty of party invites. Or better to be selective with your friend list.

Gaming with friends, Houseparty enables that. You can invite your friends to play games during chat sessions. However the games available in the room are not well developed, they have only a few rounds. So after a few rounds, you would get annoyed.

Houseparty lets you record the chat sessions, which is good to keep the memories, but it won't notify you if someone is recording your conversation, so be very careful. Also, you can record and send video messages to your contacts, you will receive a notification when they read it.

Houseparty users can keep their party private from strangers without being invited. You can create a private room by heading into Account > Settings > Private Mode.

Though Houseparty has numerous good features, but there is no monitoring by administrators. This can lead to a chance of being exposed to inappropriate content. Users can take screenshots so whatever you or other users do or posts inside the app has the potential to be seen outside of the app.



Price: Free

Overall: 9/10

SCORE

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

KEY SPECS: Available on Android, iOS, Mac and Chrome

PROS: Easy to use and connect, 8 users at a time, chat recording, supports all platforms (smartphone and PC)

CONS: Underdeveloped games, no notification when recording chat sessions

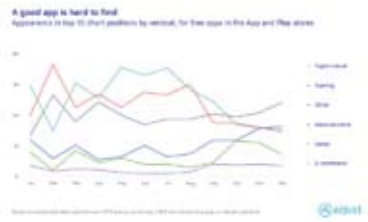
The app also has screen-sharing feature that can be used to broadcast inappropriate content. It doesn't have any kind of monitoring admins, neither parental controls or monitoring of any kind. So in case children using this app, parent should keep an eye.

The app offers various features, thus heavily consumes battery, but it's almost similar to other apps like Zoom and WhatsApp when having video call. Playing game can consumer higher amount of battery.

On different devices – The smartphone version is perfectly fine and all the functions work smoothly. But the experience is not the same. The desktop app has features but not much useful. The browser extension also lacks some of the features, so better to use it with the smartphone.

Bottomline: Houseparty has an intuitive UI that enables users to chat with your friends and family as well as play games with them simultaneously. The free app is available on all platforms, but the games are underdeveloped and for the best experience use smartphone app.

APP ECONOMY RESILIENT IN FACE OF PANDEMIC



The outbreak of COVID-19 has upended economies throughout the world, but one in particular has shown extraordinary resilience: The App Economy. Global SaaS company Adjust's annual App Trends 2020 report, which looks at long-term trends based on data from 2019, includes insights into how COVID-19 has affected the app economy by comparing Q1 2019 and Q1 2020 figures. The data shows that many app verticals are seeing increases in sessions and installs in 2020, most notably in the Business, Food & Drink, and Gaming verticals.

BING'S COVID-19 TRACKER RELEASES NEW FEATURES

Microsoft has announced new features on the Bing COVID-19 Tracker to help citizens of India stay up to date with the latest on the pandemic. These include the integration of the Apollo Hospitals bot for self-assessment and a hub for telemedicine support from reputed healthcare organizations. The Tracker will also offer content in nine Indian languages to provide people across the country access to critical information related to the pandemic in preferred language. The Bing COVID-19 Tracker serves as a single, credible hub of news and official government information. It allows users to track novel coronavirus (COVID-19) infections across the globe and in India (www.bing.com/covid/local/india) at a hyperlocal level.

KRONOS INTRODUCES EMPLOYEE CONTACT-TRACING

To aid global contact-tracing efforts and support the many essential business operations and public sector services provided by its customers, Kronos has introduced an automated reporting capability to help streamline the employee contact-tracing process, if needed, for tens of thousands of organisations worldwide. Leveraging data science to analyse labour records and time and attendance data collected by a Kronos solution, the new capability can generate a simple report, organisations can use to quickly identify and communicate to employees who may have come in contact with a co-worker who has tested positive or is presumed positive for COVID-19.

ACCOPS OFFERS FREE WFH LICENSES

To aid global contact-tracing efforts and support the many essential business operations and public sector services provided by its customers, Kronos has introduced an automated reporting capability to help streamline the employee contact-tracing process, if needed, for tens of thousands of organisations worldwide. Leveraging data science to analyse labour records and time and attendance data collected by a Kronos solution, the new capability can generate a simple report, organisations can use to quickly identify and communicate to employees who may have come in contact with a co-worker who has tested positive or is presumed positive for COVID-19.

ADMISSION24 LAUNCHES LIVE VIRTUAL CLASSES

Admission24, an EdTech Start-up Company that spruces up the idea of quality education across nooks and corners today announced the launch of its Live Virtual Classes for students and educator, as schools and educational institutions, closes across the globe due to the COVID19 pandemic. The students and teachers will get the live class timetable a day before and will get a notification 10 minutes before the class starts. By the end of the session, the students will be able to ask their queries through voice messages, text and attachment. Looking at the Internet penetration in India, the brand has also provided teachers with the option to record the class which will be available on the app for 48 hours, so that no students can miss the important session because of internet bandwidth.

peAR MAKES ITS SERVICES FREE TO RESTAURANTS

Venture Catalysts portfolio company peAR Technologies is offering restaurants free access to its contactless dine-in ordering feature. The Mumbai-based deep-tech startup has also waived off the listing charges for new restaurants. As social distancing becomes the new norm, the initiative by PeAR will enable customers to place orders from their favourite restaurants without making any physical contact.

HUAWEI'S AI-ASSISTED TECH SERVICES FOR PANDEMIC

As part of its action plan to help customers to fight COVID-19, Huawei is providing technological services in Artificial Intelligence (AI), video conferencing, wireless network coverage and smartphones to nations across Asia Pacific. Huawei has joined hands with countries like Indonesia, Malaysia, Thailand, Bangladesh and others to address on-ground communication challenges, ensuring connectivity and supporting essential services with innovative technologies during the COVID-19 pandemic.

AVITA
LIVE IT UP

Windows 10

2020 CES
Innovation Awards Honoree

ADMIROR
ECLECTICALLY EXQUISITE

PURA
SIMPLE. SENSIBLE. SASSY

WINDOWS HELLO: THE PASSWORD IS YOU.

www.avita-india.com

Toll Free: 1800-599-2273 WhatsApp: +91 7827845054

Avinash: +91 7042144117, Arun: +91 9711304064 Email: Insales@nexstgo.com

@AvitaInd @AvitaIndia @AvitaIndia

Available on amazon.in

RNI No. 45949/87 DPR No. DL(S)17/3319/2020-22 (Published on 1st of every month)
Posting Date: 3&4 every month. Posted at Lodhi Road HPO