

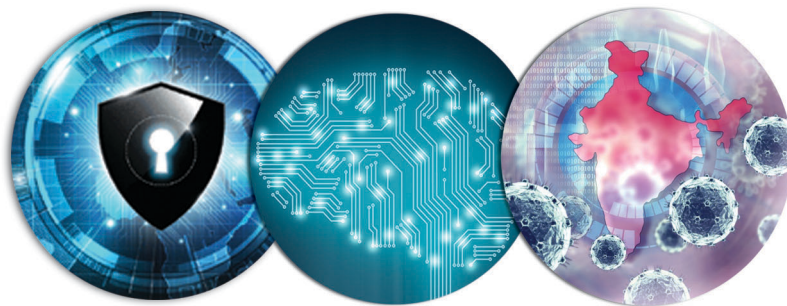


The CIOs Guide to
Serverless Computing

TOP 10 TRENDS IN
DATA & ANALYTICS

TECHNOLOGY FOR YOU

<https://www.technologyforyou.org> | June 2020 | ₹ 20



Technology to Combat
COVID-19

Artificial Intelligence
Updates



INSIDE TOPICS

COVID-19 Updates
Smartphone Tips
9 Traits for CFOs
EdTech-Key Technology
Big Data Updates
Cyber Security Updates
Top 10 Vulnerabilities
Aarogya Setu App
..Many More Articles...



Nine Future of
Work Trends

HOW BLOCKCHAIN CAN
TRANSFORM TOURISM..?



ADMISSIONS OPEN FOR 2020-21

Gwalior Bhubaneswar Noida Nellore Goa



**INDIAN INSTITUTE OF TOURISM
AND TRAVEL MANAGEMENT**

(An Autonomous Body under Ministry of Tourism, Govt. of India)

MBA*

(TOURISM & TRAVEL MANAGEMENT)
2020-22

BBA*

(TOURISM & TRAVEL)
2020-23



*under collaborative scheme of
Indira Gandhi National Tribal University

(A central university established by an Act of Parliament of India)

Degree shall be awarded by IGNTU, Amarkantak

BEST CAREER OPPORTUNITIES IN:

TOURISM BOARDS • AIRLINES/ AVIATION • RAILWAY/ IRCTC •
CRUISE/ SHIPPING • CARGO & LOGISTICS • FOREX TRADE •
BANKING & FINANCE • ADVENTURE TOUR COMPANIES •
MICE/ EVENT MANAGEMENT COMPANIES • NATIONAL PARKS •
WILDLIFE SANCTUARIES • JUNGLE SAFARIS • TOUR GUIDING

BEST CAREER OPPORTUNITIES IN:

- TOURISM BOARDS ● AIRLINES / AVIATION ● RAILWAY / IRCTC ● CRUISE / SHIPPING
- CARGO & LOGISTICS ● FOREX TRADE ● BANKING & FINANCE ● ADVENTURE
- TOUR COMPANIES ● MICE / EVENT MANAGEMENT COMPANIES ● NATIONAL PARKS
- WILDLIFE SANCTUARIES ● JUNGLE SAFARIS ● TOUR GUIDING

CONTACT DETAILS

**Exciting Careers and Excellent
Job Opportunities**

For Detailed Prospectus Please Visit

WEB: www.iittmsouth.org ; www.iittm.ac.in

Indian Institute of Tourism and Travel Management (IITTM) - Nellore

South India Campus - Golagamudi (Village & Post), via - Sarvepalli, SPSR Nellore,
Andhra Pradesh - 524 321; Mobile: 98662 74850, 94907 87854, 87781 58261,
93986 40421, 99664 62786; Phone: 0861 - 2353199; e-mail: iittmnlr@gmail.com

LAST DATE FOR APPLY - JUNE 30, 2020



TECHNOLOGY FOR YOU

TECH | CAREERS | WEB & PRINT

The Leading Technology & Career Magazine

Estd.1999 | Vol : 21 | Issue: 6 | June 2020 | ₹ 20

PRINT & WEB EDITION | www.technologyforyou.org

FOR DIGITAL SUBSCRIPTION &

For Daily Technology,
Career & Skills

Updates visit now @

WWW.TECHNOLOGYFORYOU.ORG

Honorary Editor : C. Rama Mohana Reddy

Editor in Chief : C. Janardhan Reddy

Dy. Editor. : C. Rajasekhar

Dy. Editor : B. Sravan

Associate Editor : Hussain Shaik

Editorial Staff :

C. Dharani Kumari

C. Deepika

C. Karthika

Vamshi Mohan

Bhanu Teja

Legal Advisor : Rammohan Vedantam

Senior Manager : B.E Chandra

(Space Selling)

Marketing Executive : M.K Srinivas

Photographer : Chenna Kesava

Design & Layout: S. Yadagiri

For Advertisement Support & Subscriptions :

Cell : 98496 53985, 91822 46662

Printed, Published and owned by C. Janardhan Reddy and
Printed at Bhaskar Printers, Nallakunta, Hyd. And Published at
Vidya Nagar, O.U Road Hyderabad - 44.

Editor in Chief : C.Janardhan Reddy ; All legal matters

Subject to Hyderabad jurisdiction only.

INSIDE BYTES

Serverless Computing 4

4 Key Trends for SOC...6

Five Tips to avoid COVID-19 ...8

9 Traits for CFOs ...10

EdTech Updates ... 11

Blockchain for Tourism...12

7 ethical AI principles ... 14

Tech to combat COVID-19...16

Future Work Trends ... 18

10 Data & Analytics Trends...20

Top 10 Vulnerabilities ... 22

Aarogya Setu App ... 24

Human-Computer Interaction...26

Big Data Updates ... 28

Security Updates..29 & 32

**MANY MORE ARTICLES INSIDE
TO IMPROVE TECH KNOWLEDGE....**

CONTACT US :

PLUS PUBLICATIONS

TECHNOLOGY FOR YOU

Mobile : 98496 53985, 91822 46662

e-mail : pluspublications@gmail.com

Website : www.technologyforyou.org

Add : #1-9-646-1/3, Adikmet Road, Beside SBI

Vidya Nagar, Hyderabad - 500 044

ONLINE ACCOUNT DETAILS

C.A.Name : PLUS PUBLICATIONS

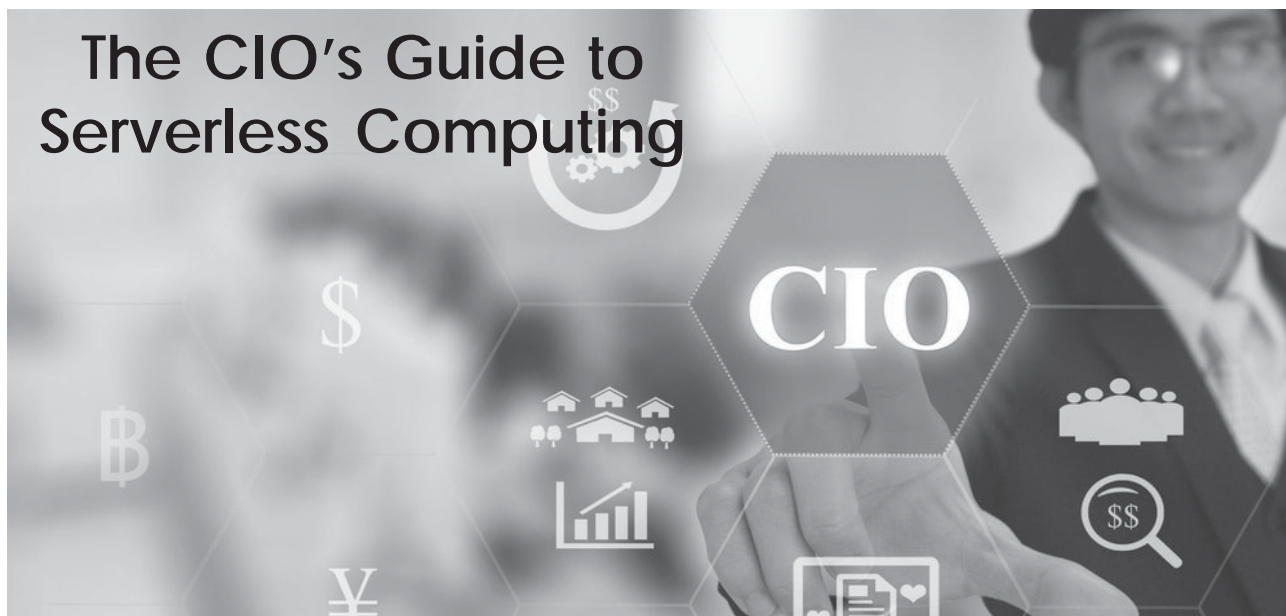
C.A. Number : 060411100001653


IFSC Code : ANDB0000604

Bank Name & Branch : Andhra Bank,
Vidyanagar, Hyderabad

FOR DAILY TECH & CAREER UPDATES VISIT @ www.technologyforyou.org

The CIO's Guide to Serverless Computing



 Serverless computing is a key technology that is redefining the way enterprises build, consume and integrate cloud-native applications.

The term “serverless computing” is a misnomer: The technology eliminates the need for infrastructure provisioning and management, but certainly does not eliminate the need for servers. It is not surprising, then, that market confusion still exists on what serverless computing is and the benefits of adopting it within an enterprise.

“Serverless architectures enable developers to focus on what they should be doing writing code and optimizing application design making way for business agility”.

Serverless computing is a next-generation technology that enables agility, elasticity and cost-effectiveness when applied to appropriate use cases. That is why CIOs building cloud computing strategies need a comprehensive understanding of the technology to dispel common myths and consider practical use cases.

What is serverless computing?

Serverless computing is a new way of building or running applications and services without having to manage the infrastructure itself. Instead, code execution is fully managed by a cloud service provider. This means that developers don't have to bother with provisioning and maintaining system and application infrastructure when deploying code. Normally, a developer would have to define a whole host of items — like database and storage capacity prior to deployment, which leads to longer provisioning windows and more operational overhead.

The most prominent manifestation of serverless computing is function platform as a service, or fPaaS. Gartner predicts that half of global enterprises will have deployed fPaaS by 2025, up from only 20% today.

The value of serverless computing

Serverless computing enables operational simplicity by removing the need for infrastructure setup, configuration, provisioning and management. Serverless computing architectures require less

overhead compared to those in which developers target the virtual machines (VMs) or containers directly.

Infrastructure is automated and elastic in serverless computing, which makes it particularly appealing for unpredictable workloads, not to mention more cost-efficient. Most importantly, serverless architectures enable developers to focus on what they should be doing — writing code and optimizing application design — making way for business agility and digital experimentation.

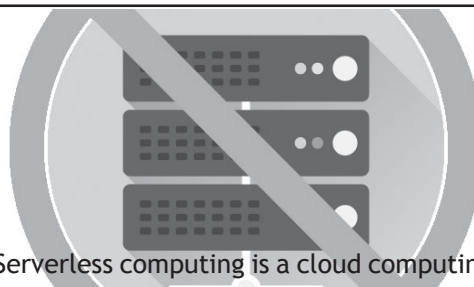
The benefits of serverless computing must be balanced against its drawbacks, including vendor-lock in, inevitable skills gaps and other architectural limitations.

Key capabilities of serverless computing

At its foundational level, serverless functions eliminate the need for end-users to manually manage the infrastructure. In turn, it provides these key capabilities:

Runs code residing as functions without the need for the user to explicitly provision or manage infrastructure such as servers, VMs and containers

Automatically provisions and scales the runtime environment, including all the necessary underlying resources (specifically the



“Serverless computing is a cloud computing execution model in which the cloud provider runs the server, and dynamically manages the allocation of machine resources. Pricing is based on the actual amount of resources consumed by an application, rather than on pre-purchased units of capacity”

compute, storage, networking and language execution environment) required to execute many concurrent function instances. Offers additional capabilities for test and development environments along with service assurance purposes, such as monitoring, logging, tracing and debugging.

How does serverless computing differ from other virtualization technologies?

VMs, containers and serverless functions have a few fundamental differences. Each approach is defined by the architectural layer that it virtualizes and how compute components are scaled in those respective environments.

Hypervisors virtualize the hardware and scale via VMs, while containers virtualize the operating system (OS). Serverless fPaaS virtualizes the runtime and scales via functions, which is why serverless solutions are suitable for projects that have specific characteristics: Runs infrequently; is tied to external events; has highly variable or unknown scaling requirements; has small and short-lived discrete functions; can operate in a stateless manner across invocations, and connects other services together.

"Each of these virtualization technologies will be relevant for CIOs in the foreseeable future," says Arun Chandrasekaran, Distinguished VP Analyst at Gartner. "Serverless, specifically, is commonly applied in use cases pertaining to cloud operations, microservices implementations and IoT platforms."

Structure your organization to take advantage of serverless fPaaS

Being "ready" for serverless fPaaS means considering three aspects of the organization:

Application development: Since operations are farther removed from visibility with serverless fPaaS, place developers and operators closer together — even on the same team — so they can share close responsibility for the development and maintenance of a software product throughout its entire life cycle.


Security and risk: The biggest change that security and risk management leaders will have to adjust to is that they no longer own or control the OS, hypervisor, container and application runtime. Instead, they can focus on areas they can control, such as integrity of code and access control.

I&O: Serverless technologies do not make other forms of infrastructure (physical machines, containers) obsolete. Most organizations will need a mix of these over time, so it's critical for I&O leaders to rethink IT operations, from infrastructure management to application governance. The role of I&O teams may be minimized in public cloud fPaaS, but ensure they work closely with developers for successful deployment.

Lessons learned for CIOs from early adopters

CIOs can shorten the learning curve and time to adoption of serverless computing by starting training on the general cloud infrastructure as a service (IaaS)/platform as a service (PaaS) environment and adopting a DevOps culture. Learning the security and technical aspects of serverless deployments is paramount, so build a proof of concept to validate assumptions about the serverless application design, code, scalability, performance and cost of ownership.

Research Finds Android handsets suffer from Region-Specific Security Issues

 Region-specific settings and configurations leave users vulnerable in some countries but not others.

Android dominates the global smartphone market and is used on many of today's most popular phones. But research from security consultants with cybersecurity provider F-Secure demonstrates that devices from some of the biggest mobile phone vendors in the world suffer from region-specific security issues that affect users in some countries but not others, resulting in a fragmented landscape of security problems.

Devices examined by the researchers include the Huawei Mate 9 Pro, the Samsung Galaxy S9, and the Xiaomi Mi 9. The exploitation process for the vulnerabilities and configuration issues, as well as the impact, varies from device to device. What makes the discoveries significant is the implication that the security of devices sold globally offers different levels of security to users in different countries. Depending on the way vendors configure devices, this can essentially lower security standards for some people but not others.

According to F-Secure Consulting's UK Director of Research James Loureiro, the presence of these security issues on popular devices expose the significant security challenges caused by the spread of customized Android implementations.

"Devices which share the same brand are assumed to run the same, irrespective of where you are in the world — however, the customization done by third-party vendors such as Samsung, Huawei and Xiaomi can leave these devices with significantly poor security dependent on what region a device is set up in or the SIM card inside of it," said Loureiro. "Specifically, we have seen devices that come with over 100 applications added by the vendor, introducing a significant attack surface that changes by region."

For example, the Samsung Galaxy S9 detects the region that the SIM card is operating in, which influences how the device behaves. F-Secure Consulting found that they could exploit an application to take full control of the device when the Samsung device's code detected a Chinese SIM card, but not SIM cards from other countries.


Research conducted on Xiaomi and Huawei mobile phones found similar issues. In both cases, the researchers were able to compromise the devices due to region-specific settings (China for the Huawei Mate 9 Pro, and China, Russia, India, and others for the Xiaomi Mi 9).

F-Secure Consulting discovered the vulnerabilities over the course of several years while conducting research in preparation for Pwn2Own — a bi-annual hacking competition where teams of hackers attempt to compromise various devices through the exploitation of previously undiscovered vulnerabilities (zero-day).

"Finding problems like these on multiple well-known handsets shows this is an area that the security community needs to look at more carefully," said Barnes. "Our research has given us a glimpse of just how problematic the proliferation of custom-Android builds can be from a security perspective. And it's really important to raise awareness of this amongst device vendors, but also large organizations with operations in several different regions."



Global Security Leaders Outline Four Key Trends for How to Transform a SOC

 Mimecast Publishes Latest Cyber Resilience Think Tank Report Concluding Technology And Automation Can Not Outweigh The Human Element.

Mimecast Limited, a leading email and data security company, today released the latest report from the Cyber Resilience Think Tank (CR Think Tank) highlighting four trends for building and operating a Security Operating Center (SOC). In the report titled, *Transforming the SOC: Building Tomorrow's Security Operations, Today*, CR Think Tank members weigh the benefits and challenges of keeping a SOC in-house versus outsourcing it. The group also lays out key actionable tips to build a successful model for any size organization.

As an independent group of security leaders dedicated to understanding the cyber resilience challenges facing organizations across the globe, the CR Think Tank provides prescriptive guidance based on lessons learned and decades of expertise. This latest report digs into the human element of team organization, various cybersecurity strategies, and the tools and technology underpinning SOC's. The CR Think Tank agreed that what works for one organization may not work for another and has identified the following trends as key factors to consider when building out a strategy for your organization:

The human element – upskilling is key

While the skill gap is clearly a challenge and it seems unlikely that any organization

will be fully staffed, the shortage does reveal an opportunity to upskill companies' existing workforces through training academies or job rotations. "The primary driver for us are skills," said Claus Tepper, head of cybersecurity operations Absa Group. "And I think South Africa is, as everywhere else, fundamentally challenged to getting the right people on board." To solve for that, Absa jumpstarted an academy to develop and train talent recognizing that it takes years for a team to become fully SOC-efficient.

In the report, all Think Tank members highlighted the importance of ensuring SOC analysts and engineers are tuned into the company's cybersecurity strategy, business processes and overall business. Malcolm Harkins, Chief Security and Trust Officer at Cymatic, believes team structures can help with upskilling: "I believe structure drives behavior," Harkins said. "We've had creative ways of getting people out of their day jobs, such as job rotations between teams, and factory tours for security and management at just the cost of time and travel, because when people understand the criticality and unique needs of a function, they're usually impressed."

In-house versus outsourced – relationships matter

Dependent on business needs, 3rd party

providers, like in other areas of the business, can be extremely valuable or, conversely, hinder progress.

When an outsourced relationship becomes a cybersecurity partnership, an external SOC team can be a key partner in addressing issues and shaping the organization's long-term security needs. However, a lack of physical presence in the office can cause miscommunication or trust issues, which are detrimental to the business.

CR Think Tank members highlights, that no matter if the SOC team is internal or external, the onus is on the CISO to showcase the SOC team's value. As that team function is not often seen as a core competency, building relationships with the senior executive leadership team will ensure CISOs have what they need for success.

Technology and automation – avoid the security chase

Automation has the potential to transform the life of a SOC analyst. Notably by increasing productivity and decreasing Mean Time to Resolution (MTTR). The experts recommend building automation into every project to make it part of the organization's structure. When it is thought about early on, automation becomes a natural part of every process. Shawn Valle,

This report highlights the potential of automation in the SOC but does warn against the over-use of it as it can make an organization's actions easier to predict and therefore more vulnerable to threat actors.

"Automation itself is a form of vulnerability," said Sam Curry, Chief Security Officer at Cybereason.

Chief Information Security Officer at Rapid7 agreed, stating: "Software developers build based on APIs, and then build UI on top of APIs, which is worthy of exploration in SecOps teams. That strategy of building automation from the beginning, we believe, makes analysts stronger and better versus using fewer people."

The report highlights the potential of automation in the SOC but does warn against the over-use of it as it can make an organization's actions easier to predict and therefore more vulnerable to threat actors. "Automation itself is a form of vulnerability," said Sam Curry, Chief Security Officer at Cybereason.

"You have to check your blind spot at pseudo-random intervals to see who's hiding there because the machine will become predictable and therefore exploitable. So, the mission is not to automate for the sake of it, but to make the humans more effective, improving the value of their output without weakening the whole."

The CR Think Tank agreed that business and security need to be in lockstep to be proactive whenever possible and avoid the security chase.

Processes and Efficiency – seating plans as the key to success?

Finally, the report highlights the importance of physical proximity when dealing with tech teams.

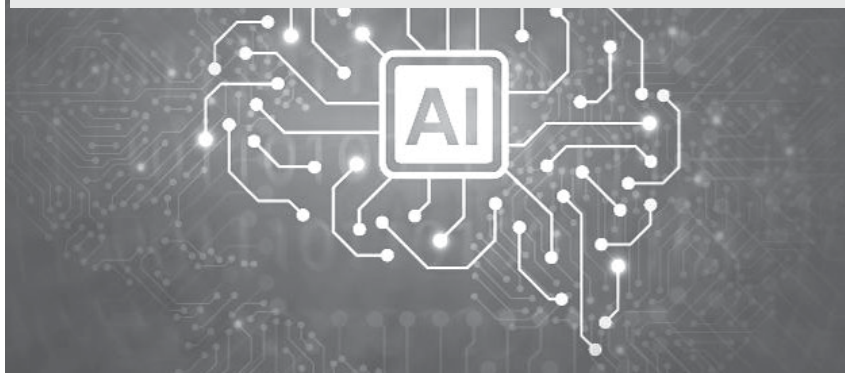
Seating location within an office can make a big difference – many companies opt to put their tech and security teams next to each other to foster creativity, agility and better communication.

For example, seating SOC teams next to the product team can improve efficiencies in terms of how they iterate and build new tools. However, for employees who work remotely, communicating with internal teams frequently to ensure alignment on priorities and objectives is key.

No matter what an organization's SOC setup is, the most important factor is relationships.

SOC teams, whether internal or external, need to be invested in the organization's mission and its core targets. With talented individuals in short supply, training, upskilling and using technology for efficiency gains are key to transform your SOC team.

88% of Security Leaders Say Supercharged AI Attacks are Inevitable



Study Finds "AI-Fueled Attacks Are Not Just Sci-Fi"

Darktrace, the cyber AI (Artificial Intelligence) company, recently announced that a commissioned study conducted by Forrester Consulting on behalf of Darktrace finds the majority of security leaders are preparing for AI-powered cyber-attacks. 88% of respondents think offensive AI is inevitable, with almost half of respondents anticipating the industry will see these attacks in the next year. With AI-powered attacks on the horizon, the report notes it "will be crucial to use AI as a force multiplier..."

Security decision-makers across a variety of industries, including retail, financial services, and manufacturing, were surveyed on the speed of attacks, the impacts of offensive AI, and businesses' security strategies in the face of advanced threats.

Key findings include:

- ▶ 88% of security leaders think offensive AI is inevitable
- ▶ 77% of respondents expect weaponized AI to lead to an increase in the scale and speed of attacks, while 66% felt that it would lead to novel attacks that no human could envision
- ▶ 75% of respondents cited system/business disruption as their top concern about weaponized AI
- ▶ Over 80% of cybersecurity decision-makers agree that organizations require advanced cybersecurity defenses to combat offensive AI
- ▶ Max Heinemeyer, Director of Threat Hunting at Darktrace, commented: I head up a team at Darktrace's R&D Center in Cambridge, where we're conducting research into AI attacks – securely developing offensive AI and using it to test and strengthen Darktrace's algorithms.
- ▶ Businesses need to implement cyber AI for defense now before offensive AI becomes mainstream. When it becomes a war of algorithms against algorithms, only autonomous response will be able to fight back at machine speeds to stop AI-augmented attacks.
- ▶ The study similarly calls for AI defenses: "If an organization is not operating with AI-enabled defenses to counter AI-enabled attacks, how can it expect to win? The goal is to fight these advanced attacks with advanced tactics that detect, interpret, and respond to the threat before it has a chance to make an impact."

"Over 80% of cybersecurity decision-makers agree that organizations require advanced cybersecurity defenses to combat offensive Artificial Intelligence (AI)"

Five tips on how to live with COVID-19



After seventy days of lockdown, the unlock 1.0 is put into action. Officially designated lockdown 5.0, from June 1, 2020, the economy and ordinary life are returning to normalcy in a controlled and phased manner. This is the beginning of a new normal. It is going to be a long haul. Experts and officials are suggesting that 'we must learn to live with the virus'. With vaccine still months away, we need to live in a new normal. Speaking to India Science Wire, Prof. K Vijay Raghavan, Principal Scientific Adviser to the Government of India, gave five tips to 'living with the virus'.

"Either we must change the virus, or we must change ourselves; changing the virus is going to take time," says Prof. Vijay Raghavan. Research and development of drugs and vaccine are underway, but for them to be available for broader use, after proper clinical trials, is going to take time. Producing the drugs and vaccine for everyone is also

time-consuming. Meanwhile, we can change ourselves to face the pandemic.

Here are the five tips from Prof. Raghavan:

► Wear a mask when you step out of the houses

Recent studies have found that when a person speaks, about 1000 tiny droplets of saliva comes out. If that person happens to be infected with novel coronavirus, then each of these droplets will carry thousands of germs. Large droplets will fall off the ground, usually within one-metre distance. However, the plum of tiny droplets can float in the air for a longer time, mainly if the area is not well ventilated. Many people who are infected by the virus do not show any symptoms. Therefore, they may not even be aware that they are affected. Wearing a mask protects not only us but others as well if we are infected. "We

have prepared a handbook on manufacturing homemade mask, which one can use to make their own face cover," says Prof. Raghavan.

► Practise vigilant hand hygiene

An analysis of 75,465 COVID-19 cases in China by a WHO-led study shows that novel coronavirus is primarily transmitted between people through respiratory droplets and contact routes. Thus, the COVID-19 virus can be transmitted when one comes into direct contact with infected people. Or when we touch surfaces in the immediate environment or objects used by the infected person (e.g., door handle and washroom tap). Our normal urge is to reach our face. When we wash our hands thoroughly with soap for at least thirty seconds, the virus, if any, on our hands is destroyed. "There are suggestions that the virus may also be transmitted by faecal and oral routes. Hence it is better to wash the hands and legs," says Prof. Raghavan.

► Maintain social distance

Most likely, the infection happens through direct contact or inhaling the droplets shed by an infected person. Droplets in usual conditions travel about a metre from the infected person. Keeping a distance of one metre from one another in markets, offices, and public transport would greatly help. "Young people can get infected without showing symptoms, and they can infect the elderly. Hence, we need to take special care to maintain physical distancing, particularly with the vulnerable like elderly, those who are ill in multiple ways," says Prof. Raghavan.

► Test and tracking

"If someone turns out to be COVID-19 positive, then one has to go back in time and identify proximal contacts of that person and identify them. We must test them," says Prof. Raghavan. Only an infected person can transmit the virus to others or contaminate a surface and spread the virus. If most of the infected persons are identified, then controlling the transmission of the virus becomes easy.

► **Isolation** - "The people who have been identified as positive cases should be isolated," says Prof. Raghavan. Once isolated, the infected person can receive proper medical attention. Further, as they remain isolated, an infected person cannot spread the virus to others. The tentacles of the infection can be cut.

"If one can do this with high speed the last one and follow all the others, then we can have a semblance of a normal life while we wait to do something for drugs and vaccine. If we don't do any of these things and if we slip upon any one of these, then we will have a problem," said Prof. Raghavan.

He also pointed out that the conditions are different in India as compared to those in western countries. Physical distancing becomes difficult as many people live in a densely populated area like Dharavi in Mumbai. Further, in India, most households have three generations living together. "This may make the implementation of physical distancing difficult. So, we need to have some innovative solutions to deal with these specific problems," says Prof. K Vijay Raghavan.

"There are multiple levels of responsibility to decide what to do. Most important of all are communication and putting the message in that communication into action by all of us" Prof K Vijay Raghavan said.

The office of the Principal Scientific Adviser to the Government of India has developed guidelines for hygiene and sanitation in densely populated areas and a manual on homemade protective covers for face and mouth. These are available for free download in many Indian languages in the website <http://psa.gov.in/information-related-covid-19>.

COVID-19 virus can be transmitted when one comes into direct contact with infected people. Or when we touch surfaces in the immediate environment or objects used by the infected person (e.g., door handle and washroom tap).

Tips to Ensure Long-Lasting Battery of Your Smartphone

Screen brightness

Reduce display levels manually to a lower level or select 'Auto' brightness adjustment option



Frequent accounts syncing

Turn off or change the setting of synchronisation for accounts



Weak/No signal areas

Avoid using the device in low or no network areas



Apps running

Close all unused apps



High consumption functions

Turn off the features such as GPS, Wi-Fi and Bluetooth when they are not in use



Genuine accessories

Always use genuine Samsung charger (Inbox item).



How to optimise & extend my battery life

Go to Settings >

- Device Care to extend battery life.
- ✓ Battery capacity and usage hours may vary depending on the device settings and usage patterns.



9 Traits for CFOs to Drive Better Performance During the COVID-19 Pandemic



Gartner, Inc. has identified nine traits CFOs should implement for better performance during the coronavirus pandemic. Gartner experts base the recommendations on findings from the past 20 years of Gartner research into how CFOs of efficient growth companies guide their organizations through periods of crisis and uncertainty.

"We're currently facing a downturn that could be even bigger than 2008 due to COVID-19," said Samantha Ellison, senior principle, advisory for the Gartner Finance practice. "CFOs and finance leaders must look carefully at these behaviors that have worked out well for CFOs after the last recession."

The nine key traits from CFOs of efficient growth companies:

1. Taking bigger, riskier growth bets

Gartner's research showed that efficient growth leaders were 1.4 times more likely to gain first-mover advantage with transformational innovations. They made M&A deals that were 21% larger and reintroduced R&D spending nearly 2 times faster than the control group. "The best-performing companies fight the tendency to hedge their bets in the growth investment process, instead of making riskier investments in identified growth opportunities," Ms. Ellison said.

2. Fighting "scope creep"

It's also important to maintain control over scale and understand the hidden cost of complexity. Gartner research has shown that efficient growth CFOs had 24% fewer

product or service lines and 18% fewer industry groups compared to their peer average.

3. Ensuring funds for critical strategic initiatives

Efficient growth CFOs build consensus on the most important strategic initiatives and make sure there are extra resources in case they are required to expand or expedite the initiatives.

4. Removing obstacles to growth bets

It's not enough to simply incentivize the right kind of risk-taking: the best-performing CFOs constantly reevaluate process and cultural "anchors" that hold back willingness to make smart growth bets. "Finance department bureaucracy is often a good place to start looking, but short-termism and 'it's-too-dangerous-to-fail' attitudes can also be anchors, as are capacity issues from ill-judged cuts," Ms. Ellison said.

5. Developing a theory of the customer

The most effective CFOs build their own hypotheses about what drives customer value instead of deferring the topic to marketing or sales. In fact, they currently spend nearly 5% of their time with customers and intend to increase that to 10%.

6. Knowing when to cut losses

An important dimension to taking bigger, riskier bets is knowing when to exit from these investments. Efficient growth CFOs

plan out timelines with associated exit triggers mapped to each stage of an initiative, long before they make such investments.

7. Protecting costs that support competitive advantages

"In particular right now, avoid spending cuts that threaten remote working," says Ms. Ellison. "CFOs should be careful they aren't cutting the very things their business needs to recover from this downturn; an indiscriminate approach to cost optimization can do that."

8. Involving the entire business in finding savings

Centralized corporate cost optimization campaigns have limits. "Finance can't always reach front-line, operational processes where efficiency opportunities may be hiding," said Ms. Ellison. "Efficient growth CFOs get creative about engaging the business in finding these savings. For example, using a system of future-winbacks to reward departments for savings found, helps to incentivize more participation in cost optimization."

9. Using a mix of budget models

Top finance teams look at different budget models to ensure they have aligned resources properly. Zero- and driver-based budget models seek to identify the activities that truly create business value.

"CFOs should seek to emulate these 9 traits of winning CFOs," said Ms. Ellison. "These proven practices have distinguished the winners from the losers after the last recession and will prepare organizations for many challenges they face today."

EdTech to remain key technology theme for India's education sector even after COVID-19 crisis



✍️ With the country expected to maintain self-isolation and social distancing practices well into the month of June 2020, when the new academic year starts for millions of students, and a few months thereafter, India's education sector is expected to witness a continued rise in the adoption of EdTech solutions, says GlobalData, a leading data, and analytics company.

The coronavirus (COVID-19) outbreak had forced educational institutions in India to suspend their operations in March 2020, when the nationwide lockdown was brought into force to prevent the spread of the virus. However, a continued rise in the number of COVID-19 cases and the lockdown extensions have left educational institutions and students worry about the continuity of learning.

Nidhi Gupta, the Technology Analyst at GlobalData, says: "A large section of students in the nation have taken to e-learning platforms amidst the COVID-19 induced lockdown to continue with their academic and other learning pursuits. High smartphone household penetration and rising broadband connectivity in the country are helping drive growth in the use of e-learning platforms among students."

This has proved to be a major shot in the arm for India's EdTech sector with most of the EdTech platforms in the country like Byju's, Coursera, Simplilearn, Toppr, UnAcademy, UpGrad, and Vedantu having seen a sharp rise in student enrolment. Various incentives offered by these companies are also attracting new users.

Byju's, for instance, has seen a massive surge in new users after it announced free access during the lockdown period. Apart from free access, EdTech companies are also modifying their offerings and introducing new features such as live interactive sessions, learning management tools, and subscription-based content, for students.

Gupta adds: "Not only has the lockdown period led to the steady rise in the adoption of EdTech solutions, but it has also brought a significant change in perception about e-learning, from what was seen as secondary learning option to now being regarded as an essential tool that can supplement or even replace traditional learning methods, particularly in times like this when the movement of students is restricted."

Not just students, even educational institutions have been proactively exploring online tutoring and remote teaching solutions from EdTech companies to enable

Many private schools have already adopted some sort of online teaching methods or the other, and are scouting for EdTech platforms offering board-prescribed syllabus that can be included for online classes. A major part of teaching for higher education in colleges and universities will also go online as they embrace digital capabilities.

seamless and uninterrupted learning and academic study for their students.

Many private schools have already adopted some sort of online teaching methods or the other, and are scouting for EdTech platforms offering board-prescribed syllabus that can be included for online classes. A major part of teaching for higher education in colleges and universities will also go online as they embrace digital capabilities.

In response, EdTech companies have started offering solutions specially designed for schools, colleges, coaching institutes and other educational institutions, enabling them to either create their own personalized platform or opt for an end-to-end online tutorial comprising free live classes and assessment tools.

India's recent decision to allow some of its universities to offer fully online degrees will also help reshape education delivery in the country. A new National Education Policy, which the government is currently working on, outlines the importance of online learning in reforming India's education system and encourages Indian institutions to not only develop their own online programs but also to recognize online programs offered by foreign institutions.

Gupta concludes: "While online learning is not new to India, the COVID-19 outbreak and the lasting impact it is likely to create is expected to drive widespread EdTech adoption not just at school and college level but also for higher education, even after the crisis is contained, making it one of the key technology themes to look out for in the country's education sector."

How Blockchain can Transform Tourism..?



By Naveen Joshi – Director at Allerin

✍ Blockchain technology is poised to revolutionize the way we travel. The use of blockchain in tourism is going to provide a new experience altogether in the way we book travel tickets and hotel rooms, providing a seamless user experience.

The global tourism market crossed USD 8 trillion in 2017. It is forecasted to have year on year growth rate of 4.7% to reach USD 11.38 trillion by 2025. The use of digital technologies like blockchain in tourism will only help in expanding the sector further. Many companies have realized the potential benefits of blockchain and have applied the technology at their workplace.

Applications of blockchain in tourism industry

Blockchain has raised a plethora of interest in the tourism industry. Many major companies have incorporated blockchain technology in their services. The following are the ways blockchain is being utilized in the tourism sector.

Decentralized payment system

Blockchain enables transportation assets to be better utilized right from the planning to the travel stage. The primary application of blockchain in tourism is to enable secure, traceable payments. The first step in international travel is booking of flight tickets. This process is relatively easy in today's age. However, the process can be simplified even further using blockchain-based methods.

Winding Tree is an open-source distribution ecosystem which facilitates

the process of booking flight and hotel tickets. It has resulted in reduced transaction costs up to 20% for consumers availing blockchain facility for ticket bookings. Airline companies like Air New Zealand have incorporated blockchain technology, making the ticket sales process less complicated. It can also help prevent over boarding of flights. Payments for the services can be made quickly and securely using blockchain methods. Thus, it enables faster checkout during transactions.

Blockchain uses cryptocurrencies like Bitcoin, which eliminates the need for using digital payment methods that rely on third-party payment apps.. The payment can be made between the two parties involved directly. This forgoes the need for a payment merchant altogether. The need for payment gateway companies like Visa and MasterCard may become obsolete because of blockchain technology.

A future where a person walks into an airport and directly boards a flight without having to stand in queues for verification or even letting go of third party apps like Expedia to get the best deal will be possible because of blockchain technology. Private cab aggregators like Uber and Lyft will only help drive the technology forward.

Blockchain-based payments will help minimize the time taken for the completion of payments. It will also facilitate payments for customers using autonomous cab services. Transactions are completed by deducting the amount automatically from the user's digital currency.

Governments can also utilize blockchain technology to provide a quicker, secure

experience for people using public modes of transport. The need for a physical rail and bus ticket can be eliminated due to blockchain and AI technologies. A single database would be sufficient to map a user's travel across all modes of services used by the customer. A single identification and payment method will be sufficient to avail the various public transportation services. Governments can also regulate private transportation services by incorporating them into the blockchain system. The payments can also be made easily using blockchain on a daily or monthly basis at the user's convenience.

Another area in which blockchain is useful is eliminating the need for physical contracts. Blockchain lets go of physical documentation, replacing it with digital ones. Digital contracts are signed, which are time-saving and can also be helpful in case of a dispute. A digital copy of the agreement can be used by the consumer to understand the terms and conditions stated by the service provider.

Customer Identification

Customer identification is crucial for the travel and tourism industry. Immigration officials must verify the identity of every foreign tourist for security reasons. Blockchain has the potential to transform the current practices for verification of travelers. The present scenario requires a traveler to produce identification at multiple stages like airport check-in and immigration.. This results in significant wastage of time, which accumulates at every stage. . Blockchain will reduce the time spent for customer verification at immigration, check-in times at hotels, long queues at embassies, facilitating a time-efficient experience. The need for a passport may also be eliminated if international governments adopt blockchain technology for their tourism industry. However, this seems a bit far-fetched as it will be hard for major countries to adopt blockchain technologies. ShoCard is a digital identity platform built on blockchain to authenticate people without usernames and passwords. Blockchain eliminates the need for the username and password methodology used for digital payments. The system is also more secure as it doesn't contain a central database, which the hackers can exploit.

Baggage management

Baggage handling is one of the critical aspects of the aviation sector. Instances of misappropriation of baggage is a significant issue faced today. Baggage mishandling and loss is a common concern today for airline companies. International baggage has to change multiple hands during transportation. The luggage is misplaced in transit due to human error. Baggage loss or mishandling can be reduced significantly using blockchain and other technologies. Blockchain data can be used to identify and monitor luggage. It can be used with AI and sensor technologies to determine the location of the baggage, in case it gets misplaced. Sensors can be attached to bags to track their exact location even if the handlers misplace it. The use of blockchain in tourism for baggage management helps eliminate the baggage loss issues faced in the industry today.

Customer rewards system

Travel service providers run loyalty schemes to encourage returning customers. Blockchain can assist with these programs, allowing customers to access their loyalty rewards easily. Services using blockchain can reward the customer with cryptocurrencies, which can be used for future travel. They also eliminate the need for a third-party mediator platform. Services like Trippki uses a loyalty reward system for their customers. Customers are allocated crypto tokens for staying in hotels. These tokens are permanently recorded in the blockchain which can be used during future transactions. The use of blockchain in tourism helps companies retain customers and increase their revenues. It also helps combat fraud in this field as the blockchain data cannot be manipulated.

Transparent business ratings

People are increasingly using the internet to check forums and read user reviews before traveling. However, their accuracy cannot always be guaranteed. Many businesses put up fake reviews for themselves as well as their competitors. These fraudulent activities have become more rampant because of increased competition. This has led businesses to adopt illegal activities to promote their businesses. The users' experience may be completely different than what they may have imagined from reading reviews online. It reduces the trust a user has with regards to other online reviews that he may encounter. Data stored on blockchain is highly secure, which enables greater transparency and consumer trust.



Traveler Tips to Protect Your Devices Data and Privacy

Most vacationers are concerned with sunscreen, passports, and phone chargers, and cyber criminals are the farthest thing from their minds. In fact, 73 percent of traveling people don't use a Virtual Private Network (VPN) to protect their internet connection, and a whopping 92 percent potentially put their personal information at risk while using public Wi-Fi.

"In this connected world, it's not enough to just lock up the house. It's important to carefully protect everything from your identity and privacy to your data and devices while on vacation."

Norton by Symantec recommends travelers follow the below guidelines to help protect their devices, data and privacy during vacation.

► **Beware of online travel scams:** Travel deals that appear too good to be true usually are. Use the official website of the hotel, airline or rental car company to book your reservations. If you're not sure it's the right website, call the company to verify.

► **Don't broadcast your plans or locations:** Vacation photos are an advertisement you're gone. First, update your privacy settings on social media to ensure only trusted friends and family can view your profile. Even then, avoid sharing specific dates. Never post pictures of itineraries or flight tickets. And remember: a harmless photo tagged to Antigua immediately alerts criminals to your empty home.

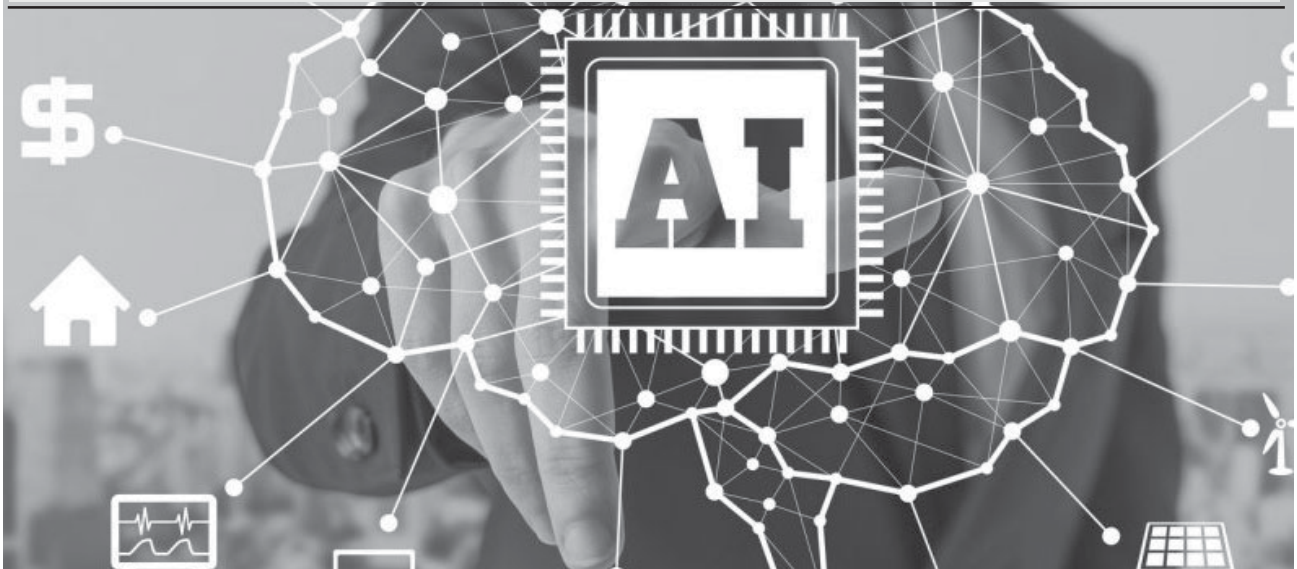
► **Surf safely:** It's easy to let your guard down when entering the plush lobby of a beautiful resort. If possible, avoid connecting to public Wi-Fi at hotels, airports, or in restaurants. Anyone sitting nearby with simple hacking equipment can see and grab the logins, passwords, and data you type or see on your screen while surfing the web. When you do connect, use a trusted VPN to connect to the Internet. This will help encrypt all communication so attackers can't view it.

► **Leave Bluetooth behind:** Bluetooth is great in the car or at home, where it's safe to communicate with other electronic devices. However, most of us forget to turn Bluetooth off when in public places, especially on vacation. With Bluetooth connectivity left open, anyone sitting in a hotel lobby or nearby coffee shop can potentially pick up that signal and gain access to your phone. It happens suddenly and without your knowledge. So say goodbye to Bluetooth while on vacation.


► **Use a credit card instead of a debit card:** You're not held responsible for unauthorized credit card purchases (beyond a nominal fee in some cases), but a thief armed with your stolen debit card information could wipe out your entire bank balance, at least until an investigation is completed. Even better, consider using an online or mobile payment service such as Apple Pay, Android Pay or PayPal.

► **Remain vigilant when it comes to your credit cards:** Before you go on vacation, alert your credit card companies to your travel plans and monitor your accounts daily for suspicious activity. During your trip, only use the credit cards and IDs that are absolutely necessary and secure your devices in the hotel safe. In addition to pick pocketing, thieves target travelers via card skimmers at gas pumps and ATMs. Skimmers are on the rise, stealing credit card or debit card information from unknowing travelers. Often, inspecting an ATM or gas station pump will not help you identify the skimmers that are placed inside the terminals. With gas stations, many times the skimmer is inside the pump making it virtually impossible to see.

7 ethical principles Artificial Intelligence developers need to follow



by Naveen Joshi
Founder & CEO - Allerin, Mumbai

 Developers need to create AI solutions by keeping in mind certain AI principles to reap the technology's benefits without incurring its inherent risks.

Artificial intelligence (AI) has progressed by leaps and bounds in the past few years. The solutions that can be created with artificial intelligence technologies are unimaginable. However, there is a possibility that artificial intelligence systems will progress to the point where they will be capable of making complex decisions in a matter of seconds with full autonomy. The dark side of such advancement is that the technology will

attain complete autonomy, override human decisions, and potentially cause harm to mankind. Scenarios demonstrated in movies such as *The Terminator*, *Wall-E*, *2001: A space odyssey*, and *Avengers: Age of Ultron*, where artificial intelligence systems turn evil, may become a reality if the technology isn't checked. Thus, regulating the potentially limitless capabilities of artificial intelligence technology becomes necessary. For that, developers need to meet a certain set of AI principles that ensures that ethics aren't compromised during the life cycle of the AI system. This ensures that the AI system doesn't harm any individual and prevents it from going rogue. These principles can help reduce security risks, improve confidence among users, and help achieve better adoption and outcomes with AI solutions.

Ethical AI principles developers need to follow

While developing AI solutions, developers need to follow certain principles to ensure that the safety and security of the software aren't compromised, and the software benefits one and all. Some of the principles developers can focus on include:

1. Human-centricity

When conceptualizing an AI solution, developers should go ahead with the

development, only if the AI system benefits individuals, enterprises, and the human race as a whole during its entire life cycle. AI solutions should be developed for primarily benefitting and improving human life, instead of achieving destructive ends. The AI systems should be aligned with human values, promoting human rights, respecting individual opinions, improving the standard of living, saving human lives, and even protecting the environment.

The education and healthcare sector are the two most important sectors which can benefit from a human-centric approach with AI technologies. AI solutions can help improve the quality of education, which will help students find better job opportunities, which, in turn, will help improve the quality of life of such individuals. Similarly, the use of AI technologies in the healthcare industry can potentially help save lives.

However, the use of AI technologies should not be restricted to these two sectors and can be leveraged in other areas such as enterprise resource planning, oil and gas operations, entertainment, and environmental protection.

2. Risk awareness

A risk-based approach should be adopted when creating an AI system. Developers should identify all the risks associated with specific AI systems. And they should only proceed with the development of the AI system if the risks are insignificant or non-existent. For instance, when developers are working with facial recognition technology, they should assess all the things that can go wrong with the technology. They should ensure that facial recognition technology does not harm any individual.

For example, facial recognition technology isn't foolproof and has resulted in false convictions. Thus, developers, when creating such a system, should ensure that the technology has as few risks associated with it as possible. Developers should, thus, not turn a blind eye to risk awareness, assessment, and management when working with AI technology.

3. Reliability

As mentioned above, AI systems should have as few risks associated with them as possible. Developers should aim at creating highly reliable AI solutions. The solutions should work as intended throughout their lifecycle. It includes ensuring that the solutions are highly accurate, reliable, and predictable at every stage.

They should not pose risks to users that might get affected by these systems. And thus, developers should ensure that the systems are monitored and tested periodically to check whether the AI solutions are working properly. If any shortcomings are found, then they should be addressed immediately. The bottom line is that developers must ensure the AI system's robustness and safety during its entire lifecycle.

4. Accountability

No matter how autonomous and self-reliant artificial intelligence technology becomes, human supervision and monitoring remain absolutely necessary. Human oversight should be enabled for AI systems, no matter how reliable or advanced the AI system is. Individuals responsible for various stages of development must be identifiable and should be held accountable for the outcomes caused by the AI system.

Mechanisms must be put in place to ensure accountability and responsibility. It includes monitoring all the processes involved, right from the conceptualization to development, and deployment to the operation phase. Appropriate actions should be taken if an individual is found responsible for the incorrect use of the AI system.

5. Compliance

AI systems should be designed to be flexible enough to adapt to new government regulations and vice versa. The AI system should be developed in such a manner that it does not require many changes to be made to comply with the new regulations. Similarly, governments should draft new laws and regulations in such a manner that the AI systems are not affected severely.

There needs to be a balance between the freedom to create new AI technology and government rules, regulations, and compliances. This can be achieved through mutual understanding,

partnership, and communication between the parties involved. Additionally, when an AI system significantly impacts an individual, enterprise, a community, or the environment, provisions should be in place that allows people to challenge the adoption, usability, and outcome of the concerned AI system.

6. Privacy

The amount of public and private data that is available to develop AI systems is scary, to say the least. Developers must ensure that privacy and data protection are respected when working with AI systems. It includes ensuring that the data generated and used by the AI systems during its lifecycle is governed and managed appropriately.

Developers must ensure that the autonomy of data and information is maintained so as not to be used inappropriately by hackers or scammers. Thus, there should be appropriate data security measures in place to protect user data and ensure privacy.



7. Cost-effectiveness - The AI systems developed should be affordable to enterprises and end-users. Developers should ensure that the AI systems are reasonably priced and can benefit a large number of people, even if the technology is proprietary. Developers can even make the technology available for free or share the source code on open-source platforms for other users to improve and build upon. The maintenance costs of AI systems, too, should be minimum. There have been questions raised regarding the ethics of AI in recent years. And rightly so.


There have been instances where AI technology has been misused or has taken decisions on its own which were questionable. And it's not just the average individual but also leaders and scientists such as Stephen Hawking, Bill Gates, and Elon Musk who have voiced valid concerns regarding AI technology. Thus, there arises a need to check AI systems. As a step in this direction, the White House has come up with its own set of AI principles that need to be followed.

These include encouraging public participation, ensuring scientific integrity and information quality, transparency, and many other principles. Developers must ensure that AI systems follow the ethics and principles outlined by the White House in addition to adherence to the ones mentioned above to ensure that their solutions are ethically sound.



Technology to combat COVID-19

by Dr. S. S. VERMA

 Technology has always helped humans to make their lives comfortable, meaningful, and powerful. Scientists and engineers are always engrossed to innovate and develop new technological ideas and devices which are changing the lives of people all over the world.

Technology only can help in making a better change in human lives going above all impediments like economic background, caste and creed, region and religion. Epidemics and pandemics has generally happened on earth from time to time but what is the difference today is the availability and use of sophisticated technologies that can, and in a lot of ways are, proving to be critical in combating the Coronavirus.

Thanks to technological advancements that we are more equipped than any era in the history to respond to a pandemic. In the present times when the world is facing an unprecedented challenge to fight against coronavirus COVID-19, people are again looking towards affordable, fast, favorable, suitable and useful technological developments. The development and access to new technology will not only accelerate combating the current pandemic but new technology and scientific discovery will also enable and better prepare the society for future crises. Further, sharing expertise, resources and technology can help to speed up work that is going to save lives and expand access to critical services around the globe.

Technology underpins critical products and services that global communities, governments and healthcare organizations depend on every day. It is hoped that by harnessing the expertise, resources, technology and talents, can help save and enrich lives by solving the world's greatest challenges through the creation and development of new technology-based innovations and approaches. Development in technology will accelerate customer and partner advances in diagnosis, treatment and vaccine development, leveraging technologies such as artificial intelligence (AI), high-performance computing and edge-to-cloud service delivery. Healthcare and life sciences manufacturers will increase the availability of technology and solutions used by hospitals to diagnose and treat COVID-19. It will also support the

creation of industry alliances that accelerate worldwide capacity, capability and policy to respond to this and future pandemics.

During the time of SARS outbreak in 2002, it took scientists more than a year to decode the genome of the virus, whereas thanks to technology advancements, the Coronavirus genome was identified within a month. Had it not been with effective and advanced technology solutions, we would have been staring at an unmanageable crisis. China illustrates this case. By mustering resources at its disposal and deploying the latest technology, the country has mitigated the effects of the virus to a significant extent and profiled people at risk. Today, several affected countries are looking at the Chinese model of best use of technology to save their populations in this race against time.

Countries have used a range of technologies in their fight against the pandemic. Digital technology has been widely used to help limit the spread of coronavirus. During the COVID-19 pandemic, technologies are playing a crucial role in keeping our society functional in a time of lockdowns and quarantines. And these technologies may have a long-lasting impact beyond COVID-19. A growing number of tech companies and IT pros are working in a variety of ways to help fight the ongoing coronavirus pandemic. Here's a rundown of what some of them are doing to help fight COVID-19. Some of the new gadgets designed to fight COVID-19 has ushered in a new era of urgent innovation.

Online learning:

Initiatives taken by different industries/organizations will support education-focused nonprofit organizations and business partners to provide students without access to technology with devices and online learning resources. The initiative will enable computer availability, online virtual resources, study-at-home guides and device connectivity assistance.

Positioning technologies:

It is well known that positioning technologies play a crucial role during the time of crisis and disasters. In the case of epidemics and outbreaks too, such technologies comes in quite handy and help to track patients and affected places, thus containing the virus, apart from analyzing the pattern of the outbreak. Reliable

data and precise mapping and imagery could help towards the building of new makeshift hospitals across the country, for transportation planning, to transport essential relief goods faster, to monitor congested public areas and relaying real-time information about the pandemic safety measures to people.

Satellite monitoring:

Progress at various sectors involving in pandemic combating can be continuously monitored using a constellation of high-resolution earth observation satellites.

Robotics:

From preparing meals at hospitals, doubling up as waiters in restaurants, spraying disinfectants to vending rice and dispensing hand sanitizers, robots are on the frontline to prevent the spread of Coronavirus. In many hospitals, robots were also performing diagnosis and conducting thermal imaging. Robots are also being used to transport medical samples from collection site to testing labs. Smart transportation Robots carries food and medicine to patients from healthcare providers without any human contact.

Internet of Things (IoT):

Most of the devices in the hospital are coming as IoT enabled and services are carried out by robots. The initial screening of the patients is done by 5G-enabled thermometers that send instant updates. Also, there are rings and bracelets that are connected to the AI platform so that it can monitor all changes in the body.

Health sensors and apps:

Sophisticated and expansive surveillance network can be used for the public good in order to develop a color-coded health rating system that can track millions of people daily. The smartphone apps (e.g., Aarogya Setu) can warn people about the dangers of infections as well as can assign three colors to people — green, yellow and red — on the basis of their travel and medical histories. Whether a person should be quarantined or allowed in public spaces is decided based on the color code. Technology is claimed to have come up with a special facial recognition that can accurately recognize people even if they are masked. Smartphone apps are also being used to keep a tab on people's movements

Drones:

In some of the severely affected areas, where humans were at risk of catching the virus, drones came to the rescue. Drones were transporting both medical equipment and patient samples, saving time and enhancing the speed of deliveries, while preventing contamination of medical samples. Drones were also flying with QR code placards that could be scanned to register health information. Agricultural drones were spraying disinfectants in the countryside. Drones powered with facial recognition were also being used to broadcast warnings to the citizens to not step out of their homes and scold them for not wearing face masks.

Big Data and facial recognition:

Access to public information has led to the creation of dashboards that are continuously monitoring the virus. Several organizations are developing dashboards using Big Data. Face recognition and infrared temperature detection techniques have been installed in all leading cities.

and ascertain whether or not they have been in contact with an infected person.

Artificial Intelligence (AI):

With the help of data analytics and predictive models, medical professionals are able to understand more about a lot of diseases. Algorithms are available that are fighting the outbreak by predicting the structure of the virus. AI-powered infrared system can effectively screen large populations to detect change in a person's body temperature.

Autonomous vehicles:

At a time of severe crunch of healthcare professionals and the risk of people-to-people contact, autonomous vehicles are proving to be of great utility in delivering essential goods like medicines and food items and for disinfection services.

Use of GIS:

It enables the real-time visual display of epidemic data. After the epidemic information concerning provincial and municipal health commission and emergency headquarters is released, it can be immediately mapped and the spatial, temporal and quantitative features of the epidemic data can be visually displayed on maps. This can express the geospatial positioning information of counties, townships, villages and groups, and further provide accurate base map foundation for the epidemic data-on-map within the province. Users can easily assess the epidemic risk level distribution of surroundings, city statistics, location of confirmed cases and distribution of fixed-point hospital and fever clinics. This map can provide scientific and effective technical support for the establishment of an effective early warning mechanism and prevention and control policies.

Indian groundwork:

The surge in innovation is drawing comparisons to another era of great pressure and great ingenuity. Several inventions that first saw the light of day in the white heat of that desperate global struggle have since become essential features of our daily lives. India is also making best use of technology to combat COVID-19 and the facilities available are: mapping each Covid-19 positive case using GIS, tracking health care workers using GPS and drawing up containment plan using heat mapping technologies.

Countries has sufficient preparedness in terms of hospital beds, testing kits, testing facilities, PPE, masks, ventilators etc. to deal with the COVID-19. Many Indian institutes like IITs, NITs, Engineering colleges, industries and DRDO has come forward with the development of many products for combating COVID-19. Production list of equipments for combating of COVID-19 at DRDO laboratories is as: Automatic Hand Sanitizer Dispensing Unit, Hand Surface Sanitizers, UV Based Disinfection Devices, Personnel Vehicle Area Sanitization Equipment, Sample Collection Enclosures, Hospital Aids, Mobile Labs, PPE, Robots and Miscellaneous.

While such advanced technologies have come to the rescue of millions at such a critical time, they have come at a heavy cost — as far as privacy is concerned. There is no doubt that extraordinary times call for extraordinary measures, and getting rid of the virus, saving lives and resuming normalcy is of paramount interest. This has necessitated that the contentious privacy versus security debate is not so important.

Nine Future of Work Trends Post-COVID-19



by RJ Cheremond - Gartner

✍️ As the pandemic resets major work trends, HR leaders need to rethink workforce and employee planning, management, performance and experience strategies.

The coronavirus pandemic will have a lasting impact on the future of work in nine key ways. The imperative for HR leaders is to evaluate the impact each trend will have on their organization's operations and strategic goals, identify which require immediate action and assess to what degree these trends change pre-COVID-19 strategic goals and plans.

“32% of organizations are replacing full-time employees with contingent workers as a cost-saving measure”.

“It's critical for business leaders to understand that large-scale shifts are changing how people work and how business gets done,” says Brian Kropp, Distinguished Vice President, Gartner. “HR leaders who respond effectively can ensure their organizations stand out from competitors.”

Of the nine future of work trends, some represent accelerations of existing shifts; others are new impacts not previously discussed. And in some cases, COVID-19 has forced the

pendulum of a long-observed pattern to one extreme.

No. 1: Increase in remote working

A recent Gartner poll showed that 48% of employees will likely work remotely at least part of the time after COVID-19 versus 30% before the pandemic. As organizations shift to more remote work operations, explore the critical competencies employees will need to collaborate digitally, and be prepared to adjust employee experience strategies. Consider whether and how to shift performance goal-setting and employee evaluations for a remote context.

No. 2: Expanded data collection

Gartner analysis shows that 16% of employers are using technologies more frequently to monitor their employees through methods such as virtual clocking in and out, tracking work computer usage, and monitoring employee emails or internal communications/chat. While some companies track productivity, others monitor employee engagement and well-being to better understand employee experience.

Even before the pandemic, organizations were increasingly using nontraditional employee monitoring tools, but that trend will be accelerated by new monitoring of remote workers and the collection of employee health and safety data. Make

sure to follow best practices to ensure the responsible use of employee information and analytics.

No. 3: Contingent worker expansion

expansion - The economic uncertainty of the pandemic has caused many workers to lose their jobs and exposed others for the first time to nonstandard work models. Many organizations responded to the pandemic's economic impact by reducing their contractor budgets, but there has since been a shift.

Gartner analysis shows that organizations will continue to expand their use of contingent workers to maintain more flexibility in workforce management post-COVID-19, and will consider introducing other job models they have seen during the pandemic, such as talent sharing and 80% pay for 80% work.

“Our research finds that 32% of organizations are replacing full-time employees with contingent workers as a cost-saving measure,” says Kropp. “While gig workers offer employers greater workforce management flexibility, HR leaders will need to evaluate how performance management systems apply to these workers and determine whether they will be eligible for the same benefits as their full-time peers.”

No. 4: Expanded employer role as social safety net

The pandemic has increased the trend of employers playing an expanded role in their employees' financial, physical and mental well-being. Support includes enhanced sick leave, financial assistance, adjusted hours of operation and child care provisions. Some organizations supported the community by, for instance, shifting operations to manufacturing goods or providing services to help combat the pandemic and offering community relief funds and free community services.

The current economic crisis has also pushed the bounds of how employers view the employee experience. Personal factors rather than external factors take precedence over what matters for organizations and employees alike. Employing such measures can be an effective way to promote physical health and improve the emotional well-being of employees.

No. 5: Separation of critical skills and roles

Before COVID-19, critical roles were viewed as roles with critical skills, or the capabilities an organization needed to meet its strategic goals. Now, employers are realizing that there is another category of critical roles — roles that are critical to the success of essential workflows.

To build the workforce you'll need post-pandemic, focus less on roles — which group unrelated skills — than on the skills needed to drive the organization's competitive advantage and the workflows that fuel that advantage. Encourage employees to develop critical skills that potentially open up multiple opportunities for their career development, rather than preparing for a specific next role. Offer greater career

development support to employees in critical roles who lack critical skills.

No. 6: (De-)Humanization of employees

While some organizations have recognized the humanitarian crisis of the pandemic and prioritized the well-being of employees as people over employees as workers, others have pushed employees to work in conditions that are high risk with little support — treating them as workers first and people second.

Be deliberate in which approach you take and be mindful of the effects on employee experience, which will be long-lasting. Address inequities if remote and on-site employees have been treated differently. Engage task workers in team culture and create a culture of inclusiveness.

No. 7: Emergence of new top-tier employers

Prior to COVID-19, organizations were already facing increased employee demands for transparency. Employees and prospective candidates will judge organizations by the way in which they treated employees during the pandemic. Balance the decisions made today to resolve immediate concerns during the pandemic with the long-term impact on the employment brand.

For example, advise CEOs and executive leaders on decisions regarding executive pay cuts and make sure financial impacts are absorbed by executives versus the broader employee base.

Progressive organizations communicate openly and frequently to show how they are supporting employees despite the implementation of cost-saving measures. Where feasible, look for opportunities to arrange talent-sharing partnerships with

other organizations to relocate employees displaced from their jobs by COVID-19.

No. 8: Transition from designing for efficiency to designing for resilience

A 2019 Gartner organization design survey found that 55% of organizational redesigns were focused on streamlining roles, supply chains and workflows to increase efficiency. While this approach captured efficiencies, it also created fragilities, as systems have no flexibility to respond to disruptions. Resilient organizations were better able to respond — correct course quickly with change.

To build a more responsive organization, design roles and structures around outcomes to increase agility and flexibility and formalize how processes can flex. Also, provide employees with varied, adaptive and flexible roles so they acquire cross-functional knowledge and training.

"D&I leaders will need to be involved in role design and creation of flexible work systems to ensure that employees of all backgrounds and needs are considered when the organization designs new workflows," said Ingrid Laman, Vice President, Advisory, Gartner.

No. 9: Increase in organization complexity

After the global financial crisis, global M&A activity accelerated, and many companies were nationalized to avoid failure. As the pandemic subsides, there will be a similar acceleration of M&A and the nationalization of companies. Companies will focus on expanding their geographic diversification and investment in secondary markets to mitigate and manage risk in times of disruption. This rise in the complexity of size and organizational management will create challenges for leaders as operating models evolve.

Enable business units to customize performance management, because what one part of the enterprise needs might not work elsewhere. As organizational complexity complicates career pathing, providing reskilling and career development support — for example, by developing resources and building out platforms to provide visibility into internal positions.

"To build a more responsive organization, design roles and structures around outcomes to increase agility and flexibility and formalize how processes can flex.

Also, provide employees with varied, adaptive and flexible roles so they acquire cross-functional knowledge and training"



Gartner Top 10 Trends in Data and Analytics for 2020



by Laurence Goasduff | Gartner

✍️ These trends can help data and analytics leaders navigate their COVID-19 response and recovery and prepare for a post-pandemic reset.

In response to the COVID-19 emergency, over 500 clinical trials of potential COVID-19 treatments and interventions began worldwide. The trials use a living database that compiles and curates data from trial registries and other sources. This helps medical and public health experts predict disease spread, find new treatments and plan for clinical management of the pandemic.

Data and analytics combined with artificial intelligence (AI) technologies will be paramount in the effort to predict, prepare and respond in a proactive and accelerated manner to a global crisis and its aftermath.

"To innovate their way beyond the post-COVID-19 world, data and analytics leaders require an ever-increasing velocity and scale of analysis in terms of processing and access to succeed in the face of unprecedented market shifts," says Rita Sallam, Distinguished VP Analyst, Gartner.

Here are the top 10 technology trends that data and analytics leaders should focus on as they look to make essential investments to prepare for a reset.

Trend 1: Smarter, faster, more responsible AI

By the end of 2024, 75% of enterprises will shift from piloting to operationalizing AI, driving a 5X increase in streaming data and analytics infrastructures.

Within the current pandemic context, AI techniques such as machine learning (ML), optimization and natural language processing (NLP) are providing vital insights and predictions about the spread of the virus and the effectiveness and impact of countermeasures.

Other smarter AI techniques such as reinforcement learning and distributed learning are creating more adaptable and flexible systems to handle complex business situations; for example, agent-based systems can model and stimulate complex systems.

"Responsible AI that enables model transparency is essential to protect against poor decisions".

Significant investments made in new chip architectures such as neuromorphic hardware that can be deployed on edge devices are accelerating AI and ML computations and workloads and reducing reliance on centralized systems that require high bandwidths. Eventually, this could lead to more scalable AI solutions that have higher business impact.

Responsible AI that enables model transparency is essential to protect against poor decisions. It results in better human-machine collaboration and trust for greater adoption and alignment of decisions throughout the organization.

Trend 2: Decline of the dashboard

Dynamic data stories with more automated and consumerized experiences will replace visual, point-and-click authoring and exploration. As a result, the amount of time users spend using predefined dashboards will decline. The shift to in-

context data stories means that the most relevant insights will stream to each user based on their context, role or use. These dynamic insights leverage technologies such as augmented analytics, NLP, streaming anomaly detection and collaboration.

Data and analytics leaders need to regularly evaluate their existing analytics and business intelligence (BI) tools and innovative startups offering new augmented and NLP-driven user experiences beyond the predefined dashboard.

Trend 3: Decision intelligence

By 2023, more than 33% of large organizations will have analysts practicing decision intelligence, including decision modeling. Decision intelligence brings together a number of disciplines, including decision management and decision support. It encompasses applications in the field of complex adaptive systems that bring together multiple traditional and advanced disciplines.

It provides a framework to help data and analytics leaders design, model, align, execute, monitor and tune decision models and processes in the context of business outcomes and behavior.

Explore using decision management and modeling technology when decisions need multiple logical and mathematical techniques, must be automated, or must be documented and audited.

Trend 4: X analytics

Gartner coined the term "X analytics" to be an umbrella term, where X is the data variable for a range of different structured

and unstructured content such as text analytics, video analytics, audio analytics, etc. Data and analytics leaders use X analytics to solve society's toughest challenges, including climate change, disease prevention and wildlife protection.

During the pandemic, AI has been critical in combing through thousands of research papers, news sources, social media posts and clinical trials data to help medical and public health experts predict disease spread, capacity-plan, find new treatments and identify vulnerable populations. X analytics combined with AI and other techniques such as graph analytics (another top trend) will play a key role in identifying, predicting and planning for natural disasters and other crises in the future.

Data and analytics leaders should explore X analytics capabilities available from their existing vendors, such as cloud vendors for image, video and voice analytics, but recognize that innovation will likely come from small disruptive startups and cloud providers.

Trend 5: Augmented data management: metadata is “the new black”

Augmented data management uses ML and AI techniques to optimize and improve operations. It also converts metadata from being used in auditing, lineage and reporting to powering dynamic systems.

Augmented data management products can examine large samples of operational data, including actual queries, performance data and schemas. Using the existing usage and workload data, an augmented engine can tune operations and optimize configuration, security and performance.

Data and analytics leaders should look for augmented data management enabling active metadata to simplify and consolidate their architectures, and also increase automation in their redundant data management tasks.

Trend 6: Cloud is a given

By 2022, public cloud services will be essential for 90% of data and analytics innovation.

As data and analytics moves to the cloud, data and analytics leaders still struggle to align the right services to the right use cases, which leads to unnecessary increased governance and integration overhead.

The question for data and analytics is moving from how much a given service costs to how it can meet the workload's performance requirements beyond the list price. Data and analytics leaders need to prioritize workloads that can exploit cloud capabilities and focus on cost optimization when moving to cloud.

Trend 7: Data and analytics worlds collide

Data and analytics capabilities have traditionally been considered distinct entities and managed accordingly. Vendors offering end-to-end workflows enabled by augmented analytics blur the distinction between the two markets.

The collision of data and analytics will increase interaction and collaboration between historically separate data and analytics roles. This impacts not only the technologies and capabilities provided, but also the people and processes that support and use them. The spectrum of roles will extend from traditional data and analytics roles in IT to information explorer, consumer and citizen developer as an example.

To turn the collision into a constructive convergence, incorporate both data and analytics tools and capabilities into the analytics stack. Beyond tools, focus on people and processes to foster communication and collaboration. Leverage data and analytics ecosystems enabled by an augmented approach that have the potential to deliver coherent stacks.

Trend 8: Data marketplaces and exchanges

By 2022, 35% of large organizations will be either sellers or buyers of data via formal online data marketplaces, up from 25% in 2020.

Data marketplaces and exchanges provide single platforms to consolidate third-party data offerings. These marketplaces and exchanges provide centralized availability and access (to X analytics and other unique data sets, for example) that create economies of scale to reduce costs for third-party data.

To monetize data assets through data marketplaces, data and analytics leaders should establish a fair and transparent methodology by defining a data governance principle that ecosystems partners can rely on.

Trend 9: Blockchain in data and analytics

Blockchain technologies address two challenges in data and analytics. First, blockchain provides the full lineage of assets and transactions. Second, blockchain provides transparency for complex networks of participants.

Outside of limited bitcoin and smart contract use cases, ledger database management systems (DBMSs) will provide a more attractive option for single-enterprise auditing of data sources. By 2021, Gartner estimates that most permissioned blockchain uses will be replaced by ledger DBMS products.

Data and analytics should position blockchain technologies as supplementary to their existing data management infrastructure by highlighting the capabilities mismatch between data management infrastructure and blockchain technologies.

10: Relationships from the foundation of data & analytics value

By 2023, graph technologies will facilitate rapid contextualization for decision making in 30% of organizations worldwide. Graph analytics is a set of analytic techniques that allows for the exploration of relationships between entities of interest such as organizations, people and transactions.

It helps data and analytics leaders find unknown relationships in data and review data not easily analyzed with traditional analytics.

For example, as the world scrambles to respond to current and future pandemics, graph technologies can relate entities across everything from geospatial data on people's phones to facial-recognition systems that can analyze photos to determine who might have come into contact with individuals who later tested positive for the coronavirus.

“Consider investigating how graph algorithms and technologies can improve your AI and ML initiatives”.

When combined with ML algorithms, these technologies can be used to comb through thousands of data sources and documents that could help medical and public health experts rapidly discover new possible treatments or factors that contribute to more negative outcomes for some patients.

CISA, FBI releases a list of top 10 vulnerabilities



The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government released a list today of the top 10 vulnerabilities most commonly exploited by foreign cyber actors.

The exploitation of these vulnerabilities often requires fewer resources compared to zero-day exploits for which no patches are available.

Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

According to U.S. Government technical analysis, malicious cyber actors most often exploited vulnerabilities in Microsoft's Object Linking and Embedding (OLE) technology. OLE allows documents to contain embedded content from other applications such as spreadsheets. After OLE the second-most-reported vulnerable technology was a widespread Web framework known as Apache Struts.

Of the top 10, the three vulnerabilities used most frequently across state-sponsored cyber actors from China, Iran, North Korea, and Russia are CVE-2017-11882, CVE-2017-0199, and CVE-2012-0158. All three of these vulnerabilities are related to Microsoft's OLE technology.

As of December 2019, Chinese state cyber actors were frequently exploiting the same vulnerability—CVE-2012-0158—that the U.S. Government publicly assessed in 2015 was the most used in their cyber operations. This trend suggests that organizations have not yet widely implemented

patches for this vulnerability and that Chinese state cyber actors may continue to incorporate dated flaws into their operational tradecraft as long as they remain effective.

Deploying patches often requires IT, security professionals, to balance the need to mitigate vulnerabilities with the need for keeping systems running and ensuring installed patches are compatible with other software. This can require a significant investment of effort, particularly when mitigating multiple flaws at the same time.

A U.S. industry study released in early 2019 similarly discovered that the flaws malicious cyber actors exploited the most consistently were in Microsoft and Adobe Flash products, probably because of the widespread use of these technologies. Four of the industry study's top 10 most exploited flaws also appear on this Alert's list, highlighting how U.S. Government and private-sector data sources may complement each other to enhance security.

Vulnerabilities Exploited in 2020

In addition to the top 10 vulnerabilities from 2016 to 2019 listed above, the U.S. Government has reported that the following vulnerabilities are being routinely exploited by sophisticated foreign cyber actors in 2020:

Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.

An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.

An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.

March 2020 brought an abrupt shift to work-from-home that

necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting organizations whose hasty deployment of Microsoft O365 may have led to oversights in security configurations and vulnerable to attack.

Cybersecurity weaknesses—such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans—have continued to make organizations susceptible to ransomware attacks in 2020.

Here's a comment from Satnam Narang, Staff Research Engineer at Tenable providing an analysis of a trend seen within these top 10 vulnerabilities.

CISA's list of the top 10 routinely exploited vulnerabilities from 2016 through 2019 primarily consists of flaws in Microsoft products, particularly in Microsoft Office. This comes as no surprise as cybercriminals go after low hanging fruit, which is often ubiquitous software with known but unpatched vulnerabilities. Many of the bad actors leverage flaws in Office when distributing spear-phishing emails to their intended targets. These emails are tailored to their victim, using a lure designed to capture their interest in order to convince them to open the malicious attachment.

This list is indicative of a trend we see time and time again: Cybercriminals prefer to leverage known but unpatched vulnerabilities. Finding or acquiring zero-day vulnerabilities is a costly endeavor, so leveraging unpatched flaws with publicly available exploit code gets them to their end goal in the fastest and cheapest way possible.

Vulnerabilities in Virtual Private Network (VPN) solutions are another area that has seen an increase in activity going back to 2019 when exploiting code for several notable VPNs became publicly available. We anticipate that many of these flaws will continue to be leveraged by bad actors of all kinds because as they say if it ain't broke, don't fix it.

This list is a solid reminder of the importance of basic cyber hygiene and systems maintenance. Knowing which vulnerabilities are being actively exploited by bad actors and prioritizing their remediation is one of the most effective ways to reduce risk.



Cybersecurity weaknesses such as poor employee education on social engineering attacks and a lack of system recovery and contingency plans have continued to make organizations susceptible to ransomware attacks in 2020

Open Source Software to Drive Telecom's Innovation Agenda by 2025

Open source software (OSS) serves as the foundation of IT infrastructure worldwide, allowing e-commerce platforms and innovative over the top (OTT) players to bring services to market quickly. OSS is gradually driving the innovation agenda for communications service providers (CSPs), and by extension, it is now challenging the dominance of proprietary solutions in the telecoms industry. OSS holds the potential to play a key role in telco cloud deployments, a market that will potentially grow to US\$29 billion by 2025, finds global tech market advisory firm ABI Research.

CSPs that wish to keep abreast with OTT and web-scale companies may have to implement the same technologies and agile processes to stay competitive and rapidly innovate. OSS and by extension, cloud technologies, promise nimbleness, but whether CSPs can seize the opportunity remains to be seen. Telecoms are driven by standard bodies that have long cycle times to next-generation technologies. On the other hand, open-source is characterized by an agile approach that moves faster. "Though CSPs are at different timeslots in their digitalization journey, they should collectively propel the open-source agenda forward. A close collaboration between standard bodies and open source communities is a step in that direction," says Don Alusha, Senior Analyst at ABI Research.

Furthermore, a key consideration before OSS garners vendors' support is the means of monetization. There are two main monetization models that vendors can potentially use to commercialize OSS. Namely, there is the support model and the alternative where the core of the product is open source, but vendors add proprietary bells and whistles on top. Red Hat pioneered the support model and it remains the leading vendor in commercializing OSS using that option. Other companies such as Cloudera and Hortonworks have successfully embraced underlying OSS to offer enterprise-grade modules under a commercial license.

In telecoms, the adoption of OSS is already underway among CSPs and it will almost certainly be mainstream by 2025. For example, CSPs like Orange and Bell Canada have created internal open-source groups in a bid to become more well versed in interacting with community-developed software. To that end, CSPs no longer hold reservations in adopting OSS but are now considering ways to include it in their network operations and commercial undertakings. In fact, the industry at large stands to benefit from OSS innovation with the introduction of IT and cloud solutions. But, unlike the IT domain, telecoms infrastructure is characterized by stringent performance, reliability, and security requirements that require telco-specific arrangements.

"Commercial models notwithstanding, telco vendors like Ericsson, Huawei, Nokia, and ZTE can potentially leverage OSS to realize performance and scalability as they transition their products to cloud-native equivalents. At present, OSS serves as an enablement technology for these vendors as opposed to building a business out of OSS. But eventual diffusion of 5G may well mean that vendors will need to invest significantly in open source projects to develop carrier-grade products and services in the next 5 years. When that takes place, vendors will need to channel time and investment to establish a presence in open source communities," Alusha concludes.

IT Minister Launches National Artificial Intelligence Portal of India



🗣️ The Union Minister for Electronics and IT, Law and Justice and Communications Ravi Shankar Prasad launched India's national Artificial Intelligence (AI) Portal called www.ai.gov.in.

This portal has been jointly developed by the Ministry of Electronics and IT and IT Industry. National e-Governance Division of the Ministry of Electronics and IT and NASSCOM from the IT industry will jointly run this portal. This portal shall work as a one-stop digital platform for AI-related developments in India, sharing of resources such as articles, startups, investment funds in AI, resources, companies, and educational institutions related to AI in India. The portal will also share documents, case studies, research reports, etc. It has a section about learning and new job roles related to AI.

On this occasion, the Minister for Electronics & Information Technology, Communications and Law & Justice, Ravi Shankar Prasad, also launched a National Program for the youth, "Responsible AI for Youth". The aim of this program is to give the young students of our country a platform and empower them with appropriate new age tech mindset, relevant AI skill-sets and access to required AI tool-sets to make them digitally ready for the future. The Program has been created and launched by the National e-Governance Division, Ministry of Electronics & IT in collaboration with Intel India, with support from the Department of School Education and Literacy (DoSE&L), Ministry of Human Resource Development. DoSE&L will help reach-out to State Education Departments to nominate teachers as per eligibility criteria.

"Responsible AI for Youth" will empower the youth to become AI-ready and help reduce the skill gap, while enabling youth to create meaningful social impact solutions. The Program is designed to reach out to students from Government schools pan India and provide them with an opportunity to become part of the skilled workforce in an inclusive manner.

Addressing the media at the launch event, the Union Minister for Electronics & IT, Law & Justice, Ravi Shankar Prasad said, "India must be a leading country in the development of Artificial Intelligence in the world, leveraging upon its vast Internet-savvy population and data it is creating. India's AI approach should be of inclusion and empowerment of human beings by supplementing growth and development rather than making human beings less relevant".

When connectivity is critical: 5G's call to action

🗣️ Qualcomm President Cristiano Amon discusses the importance of connectivity during these uncertain times and what 5G is bringing us.

The need for connectivity in every facet of society has never been more pressing than it is right now. This includes how we're working together throughout the Qualcomm community, as well as supporting our customers and partners around the world. More than just imagining new possibilities, people all over the world are now working beyond the office, learning beyond the classroom, and experiencing healthcare beyond the traditional doctor's office or clinic.

Cue 5G: This next generation of wireless networking is designed as the foundation for scaling connectivity and supporting mission-critical infrastructure needed across the globe. After a decade of Qualcomm Technologies breakthroughs that are leading the world to 5G, we never could have imagined that 5G would be called to action in this way. We're working closely with our customers and partners at a time when it's fundamentally important that we're all connected. We're also creating new ways to respond.

Some of the industries we're helping transform with this technology are proving to be the most vital right now. 5G networking can allow people to connect with doctors from a distance, increasing access to healthcare when it's needed most. Right now, more people are meeting with their healthcare workers over video chat, and this may become a new normal for many communities. 5G networks will enable this practice to expand, and become easier and more accessible on our mobile devices. In fact, as part of the CARES Act in the U.S., the FCC recently announced a \$200 million investment to stimulate telehealth practices and technology.

In education, the vision for 5G is to create new ways of learning, even in remote areas. Imagine students in virtual learning environments using PCs or tablets to connect and interact with a teacher in another country to learn a new language, without a lot of lag or connectivity issues.

Many of us who work in an office are likely logging on from home now, but 5G also unlocks remote work opportunities for roles beyond office jobs. For example, with 5G-connected infrastructure, workers can collaborate, while performing data-intensive tasks. Imagine scientists collecting data in the field while video chatting with colleagues who are analyzing that same information in real-time. This is just one example of how 5G can pick up the pace of human innovation in ways that matter most.

These times are shining the spotlight on our ability to work remotely and, above all, remain connected and collaborate. We're hearing a lot of excitement from the mobile network operators we work with, as they continue to pursue 5G plans.

And Qualcomm will do its part, too. Now, more than ever, we remain dedicated to creating breakthrough technologies that can help the world connect, compute, and communicate for the better.

Aarogya Setu App is now open source

On 2nd April 2020, India launched Aarogya Setu mobile App for helping augment the efforts of limiting the spread of COVID19, with an objective of enabling Bluetooth based contact tracing, mapping of likely hotspots and dissemination of relevant information about COVID19.

The App has over 114 million users as on 26th May, which is more than any other Contact Tracing App in the world. The App is available in 12 languages and on Android, iOS, and KaiOS platforms. Citizens across the country are using Aarogya Setu to protect themselves, their loved ones, and the nation. Many youngsters also call Setu as their Bodyguards.

The key pillars of Aarogya Setu have been transparency, privacy, and security and in line with India's policy on Open Source Software, the source code of Aarogya Setu has now been made open source. The source code for the Android version of the application is available for review and collaboration at https://github.com/nic-delhi/AarogyaSetu_Android.git. The iOS version of the application will be released as open-source within the next two weeks and the server code will be released subsequently. Almost 98% of Aarogya Setu Users are on the Android platform.

Opening the source code to the developer community signifies our continuing commitment to the principles of transparency and collaboration. Aarogya Setu's development has been a remarkable example of collaboration between Government, Industry and Academia, and citizens. It is also a product of the hard work of the talented young technological experts of our country who have worked a day in and out to make this world-class product. With the release of the source code in the public domain, we are looking to expanding collaboration and to leverage the expertise of top technical brains amongst the talented youth and citizens of our nation and to collectively build a robust and secure technology solution to help support the work of frontline health workers in fighting this pandemic together.

The App offers a comprehensive suite of

interventions against COVID-19 and has registered several firsts in the eight weeks since its launch. The App possibly has the most reach and impact when compared to all other COVID-19 contact tracing and self-assessment tools combined globally, while pioneering new data-driven epidemiological flattening of the curve through syndromic mapping. Of the more than 114 million registered users, two-thirds have taken the self-assessment test to evaluate their risk of exposure to COVID-19. The App has helped identify about 500,000 Bluetooth contacts.

Those who are identified as Bluetooth contacts of COVID19 positive cases or are classified as needing assistance based on their self-assessment, are contacted by National Health Authority. So far, the platform has reached out to more than 900,000 users and helped advise them for Quarantine, caution, or testing. Amongst those who were recommended for testing for COVID19, it has been found that almost 24% of them have been found COVID19 positive. Compare this to the overall COVID19 positive rate of around 4.65% – 145380 COVID19 positives from a total of 3126119 tests done as on 26th May 2020.

This clearly illustrates that Contact tracing is helping focus efforts on those who need testing and this will greatly augment the efforts of the Government in containing the pandemic. Analytics of Bluetooth contacts and location data has also helped identify potential hotspots with a higher probability of COVID cases allowing State Governments and District Administration and Health authorities to take necessary steps for containment of the pandemic, early, which is critical for controlling the spread of the pandemic. This approach of syndromic mapping, a novel approach of combining principles of path tracing and movement patterns of COVID-19 positive people, population-level epidemiology modelling and the prevalence of COVID-19 in different regions of the country, the Aarogya Setu team has identified more than 3,500 hotspots across the country at the sub-post office level.

The Aarogya Setu data fused with historic data has shown enormous potential in

predicting emerging hotspots at the sub-post office level and today around 1264 emerging hotspots have been identified across India that might otherwise have been missed. Several of these predicted hotspots have been subsequently verified as actual hotspots in the next 17 to 25 days. As an example, a district with 3 cases on a particular date when the Aarogya Setu engine predicted it as a hotspot registered 82 cases in the next 15 days. The precision achieved by this unique combination of Bluetooth-based contact tracing and identification of hotspots may hold the key to effectively breaking the chain of infection, flattening the curve, and saving lives.

Releasing the source code of a rapidly evolving product that is being regularly used by more than 114 million users, is challenging. Developing and maintaining the source code is a huge responsibility, both for Team Aarogya Setu and the developer community. The repository now being shared is the actual production environment. All subsequent product updates will also be made available through this repository.


The process of supporting the open-source development will be managed by National Informatics Centre (NIC). All code suggestions will be processed through pull request reviews. Aarogya Setu's source code has been licensed under Apache License.

Version 2.0, and is available on an "As-Is" basis. Any reuse of the source code with changes to the code requires the developer to carry a notice of the change. More details can be found in the Frequently Asked Questions document available at <https://www.mygov.in/aarogya-setu-app/>.

While making the code Open Source, the Government of India also seeks the developer community to help identify any vulnerabilities or code improvement in order to make Aarogya Setu more robust and secure. Towards this objective, the Government has also launched a Bug Bounty Programme with a goal to partner with security researchers and the Indian developer community to test the security effectiveness of Aarogya Setu and also to improve or enhance its security and build user's trust. Details of the Bug Bounty Programme along with the rewards therein are being shared separately. Details of the Bug Bounty Program is available on the innovate portal of MyGov at <https://innovate.mygov.in/>



How human-computer interaction increases worker productivity

 The constant evolution in human-computer interaction is assisting workers with their daily operations to increase their productivity.

Humans have long been developing tools and technologies that can assist them in their daily tasks. Computers are one such tool that have changed the way humans work. Human-computer interaction (HCI) focuses majorly on the study of interfaces that allows interaction between people and computers. The field of HCI is situated at the intersection of computer science and behavioral science. HCI has evolved over time, from desktops to mobile screens and handheld computers. Present-day research focuses on seamless implementation with voice user interface and speech recognition. This evolution, over time, has assisted humans in their daily operations by reducing the burden and increasing productivity. For instance, chatbots are an example of how human-computer interaction has enhanced worker productivity.

Technologies that will increase productivity through human-computer interaction

Advancement in technologies has paved the way for several tools and devices like eye-trackers, wearables, and virtual assistants that have facilitated human-computer interaction.

Eye-tracking

Eye-tracking is the process of interpreting where a person is looking, also known as the point of gaze. Eye-attached tracking, optical tracking, and electric potential measurement are three techniques to track eye-movement. The first technique uses an attachment with an embedded mirror or magnetic field sensor to track the eye. Optical tracking is done with the help of infrared rays and their reflections detected with the help of infrared cameras. The electric potential measurement uses electrodes to determine eye movement.

Business administrators can help workers focus on their daily operations with the help of eye-tracking. For instance, eye-tracking devices can determine industrial processes or situations that divert workers' attention. Businesses can then make plans or strategies that can help tackle distractions and enhance workers' focus on a task. Eye-tracking also helps to train employees. It can record the visual attention of an expert while he or she is performing a task. And this recording can help train new employees about what to look and where to look while performing a task. Thus using eye-tracking technology and human interaction with its devices helps new employees to learn everything from an expert's perspective without missing a single detail. Eye-tracking in the future might also eliminate

the need to scroll down the computer screens manually, which will further increase worker productivity. For instance, front-desk receptionists can simply scroll computer screens with their eyes and focus more on assisting customers with other tasks and queries.

Speech recognition

Speech recognition technology can interpret human language, and it is already in use to increase productivity with chatbots and virtual assistants. Chatbots can understand customer queries and provide an appropriate response. Thus, with chatbots to solve customer queries, workers can focus more on decision-making tasks. And chatbots are just one of the many applications of speech recognition that can increase workers' productivity. Simply putting it can assist in all the typing tasks, be it personal or professional. According to a report, an average person types 40 words per minute, and a professional typist can type around 60 to 80 words per minute. Another report shows that an average person speaks between 120 to 150 words per minute. Comparison between both the report shows that the speaking rate is almost twice the typing rate. Thus, it can double the productivity of typing tasks.

It can also increase the productivity of non-typing tasks. For instance, it can help take down even minute details of all

transcribing meetings, training sessions, interviews, and presentations. Also, accountants can update accounts in a computer device by simply reading them without the need to type anything.

IoT (Internet of Things)

IoT applications are penetrating their way into our daily lives and almost all the industries. IoT devices collect data that can provide valuable insights to businesses and helps them to make significant decisions for increasing their revenues. But IoT devices are not all about collecting data, human interaction with these devices can also help increase workers' productivity. Time management is important and can have a significant impact on employees' performance. It can help an employee provide better quality work, make better decisions, eliminate procrastination, and reduce stress and anxiety.

IoT devices can help employees to manage their time efficiently. For instance, wearables, like smartwatches, can have applications such as scheduling, taking notes, and reminders that can help employees remember minute details, manage their time and increase their productivity.

Cloud computing

Imagine a workplace of twenty years from now; it will be completely different from today. Businesses are taking a paradigm shift towards becoming a remote workplace. Employees themselves prefer working remotely. For instance, According to a survey done, 83% of workers do not believe they have to be in an office to be productive. And the same study shows that 43% of workers feel they would be more productive working from home. Thus employees want flexibility in their way of working, which can be achieved with innovative technologies. And this remote workforce becomes possible because of cloud computing and human interaction with mobile devices to access cloud-based business applications.

Cloud-based SaaS (Software as a Service) applications can enable seamless collaboration and streamline workflow to increase workers' productivity. Any employee who has been granted permission can access the data on the cloud from anywhere in the

world and establish real-time communication with fellow employees. And these collaborative technologies can allow communication between remote teams and help to increase productivity. Hence, it can be said that the future workforce will shift from location-centric to work-oriented because of SaaS and human-computer interaction.

AR/VR

Immersive technologies like AR and VR connect humans to the digital world and assist them while performing daily operations to increase productivity. Smart glasses allow workers to interact with computers in a fascinating hands-free way. And when combined with other technologies like cloud-based services and mobile applications, these smart glasses can provide critical information to workers while they are performing their daily tasks.

Smart glass technology has progressed rapidly in recent years. There are many vendors providing smart glasses with different features such as see-through displays, HD cameras, and voice- and gesture-activated controls. And this progress in smart glasses has allowed workers to interact with computers seamlessly. They also allow workers to learn on the job. For instance, a chef can learn new recipes and simultaneously prepare them. Also, they can help reduce downtime. By having AR and VR apps, the maintenance team can visually identify problems in machinery and resolve them there and then.

Learning with the help of AR and VR helps workers to enhance their accuracy and quality of work, and ensures that the task is completed with zero errors. Thus, it reduces the time required for rework and leaves workers with ample time to focus on other tasks and increase productivity.

The current research in HCI is focused on user customization, sentiment analysis, and brain-computer interfaces. When researchers and developers find new breakthroughs in the above areas, they can create HCI tools that can be tailored according to workers' needs to make them more productive. For instance, if a worker is not efficient enough to do accounts, then human-computer interaction tools can be tailored to focus more on assisting with accounts for that worker.

Human Computer Interaction

Human-computer interaction (HCI) is a multidisciplinary field of study focusing on the design of computer technology and, in particular, the interaction between humans (the users) and computers. While initially concerned with computers, HCI has since expanded to cover almost all forms of information technology design.

In summary, HCI focuses on increasing user effectiveness and improving user computer experiences with organizational systems. It does so by enhancing the user interface through an understanding of the tasks and organizational contexts in which HCI occurs.

The goal of HCI is to improve the interaction between users and computers by making computers more user-friendly and receptive to the user's needs.

The main advantages of HCI are simplicity, ease of deployment & operations and cost savings – for smaller set-ups. By using HCI you have fewer systems to manage. The hyper-converged clouds reduce the time required to deploy many applications. They also reduce solution design time and integration complexity.

Human-Computer Interaction (HCI) is the study of how people interact with computers and to what extent computers are or are not developed for successful interaction with human beings. HCI concerns the design, evaluation and implementation of interactive usable user interfaces.



How Big Data can drive mobile applications



 **by Naveen Joshi-Director at Allerin. Process Automation, Connected Infrastructure (IoT). R & D on ML/DL.**

Businesses and developers can leverage big data in mobile app development to understand end-users, develop marketing strategies, and generate more revenue.

According to a study, 63% of customers want personalized product recommendations. In today's world, where customers themselves prefer personalized product recommendations, big data helps in understanding them and creating those tailored products. These products, among other things, also include software like web-based applications. As a result, developers do not have to put in much of their own thoughts and creativity for developing a web-based application as they can process a huge amount of data to understand what customers need. And this understanding helps in faster web-based application development.

Big data also facilitates better and accurate traffic analysis that further helps in developing strategies to improve applications. But now, mobile application adoption is growing. According to a survey, 204 billion apps were downloaded worldwide in 2019. And that doesn't come as a surprise because every web-based application available today can be easily converted to a mobile application. There are also several applications that are developed solely for mobile and do not exist as web-based applications. Mobile applications also provide additional benefits over web applications. For

instance, mobile applications can track users' live location, fitness data if linked to a wearable, and provide real-time collaboration with them. Businesses can leverage big data in mobile app development to combine the benefits provided by each of them.

The role of big data in mobile app development

Mobile app developers can use big data for understanding end-users and creating marketing strategies accordingly. They can also provide personalized recommendations to customers based on preferences, demographics, and locations.

Marketing products

Mobile applications allow businesses to pitch in their products through push or email notifications. But, they cannot send notifications for any random products. Real-time big data access will help businesses to understand what products to pitch in through push notifications at the right time. Big data also provides opportunities for businesses to understand customers' needs and offer tailored products. It also helps to create marketing strategies about what kind of email notifications to send to users.

Understanding end-users

With the availability of big data about

preferences, demographics, and locations of end-users, developers can understand their needs. Big data also fuels developing user experience analytics. And based on the experience analytics, developers can create app updates to enhance the user interface. Changing the user interface based on experience analytics enhances user engagement.

Improving decision-making


As the saying goes, that, "smart decisions are made between choosing what you want now and what you want in the future." And big data is a culmination of business intelligence and predictive analytics. Big data and IoT devices (smartphones) can together provide access to real-time data for predictive analytics that can help to make and improve strategic decision-making.

Big data is an inevitable part of today's life, where providing tailored products has become an essential key to business growth. Business giants are already using big data in mobile app development and engagement with users. For instance, Uber is using big data for its mobile application to connect users with drivers in their location and calculate pricing based on travel distance. Amazon as well utilizes big data to know what items a client has purchased before, and provide recommendations of similar and relevant products.

"Mobile app developers can use big data for understanding end-users and creating marketing strategies accordingly. They can also provide personalized recommendations to customers based on preferences, demographics, and locations"

New Survey Reveals Cybersecurity Training is Missing the Mark as Employees Work around Company Security Policies



 With Global Cybersecurity Threats On The Rise, Investment In Security Training Is Essential To Drive Cultural Change And Business Success.

Mimecast Limited, a leading email, and data security company, today released a study titled *Don't Just Educate: Create Cybersafe Behaviour*. The survey shows that while customer data breaches and reputational damage around the world is encouraging businesses to re-examine their security practices, employee cyber behavior still needs to change.

The survey, conducted by Forrester Consulting, found that while 59% of security and IT managers think they are 'ticking the security compliance box', their employees report a huge disconnect. More than half of the 240 employees surveyed in APAC (53%) disagree with that statement, and 51% believe their managers do not stress the importance of good security practices.

The survey was conducted across Australia, Hong Kong, New Zealand, and Singapore between January and February 2020 and involved 120 senior IT and business decision-makers responsible for cyber safety at companies with more than 100 employees. Respondents represented 20 industry sectors including government, healthcare, legal, marketing, energy, telecommunications, transport, and logistics.

The survey included a wide range of questions around Security Awareness and Training (SA&T) Programs in APAC, including security measure and implementation, employee behavior changes, security culture, and overall effectiveness in delivering effective training programs. Results of the employer survey were measured against feedback from 240 knowledge workers within these companies, who regularly use email and digital channels in the workplace.

Across the region, the study also found that attending SA&T activities does not necessarily translate to a change in behavior for employees, with a third of SA&T attendees still admitting to flouting security policies — increasing to more than 50% for respondents in New Zealand.

"While security leaders in APAC believe they've made security a social norm by leading and encouraging others, this survey

underscores that employees are not retaining, understanding or implementing key areas of cybersecurity training – and the existing outdated modes of training are simply not bringing about behavioral change," said Nick Lennon, Country Manager for Mimecast Australia and New Zealand.

"In the current COVID-19 business conditions, with many employees working remotely indefinitely, the last thing businesses need is a security breach."

Additional findings from the Forrester Consulting study include:

Traditional SA&T is long and unengaging, uses outdated content types, and does not rely on behavioral science to achieve its objectives of behavior and culture change.

As a result, employees' behaviors are not changing, which further contributes to a disconnect between employers' perceptions and how their employees really feel about security.

APAC firms must advance SA&T programs by exploring alternative content types, providing different methods of delivery based on employee preferences, and extending training outside the workplace.

"Almost half of business leadership teams (45%) still have the incorrect perception that security impedes their workforce productivity," as noted in the study by Line Larrivaud, Forrester Consulting Project Director for this survey. At the same time, she notes that "Attending SA&T activities does not necessarily translate into a change in behavior for employees — with 31% of training attendees in APAC still admitting to going around security policies. In New Zealand, more than half (52%) admitted to this".

"At a time when global cybersecurity threats, customer data breaches, and the potential for reputational damage has never been greater, it's of vital importance that business leaders and employees understand and value the importance of cybersecurity best practice within their organization. They simply cannot ignore the consequences or circumvent the protocols," commented Lennon.

Legacy Technology & Lack of Skills Hindering Digital Transformation and IT Modernization



 Veeam 2020 Data Protection Trends Report indicates global businesses are embracing Digital Transformation, but struggle with antiquated solutions to protect and manage their data; data protection must move to a higher state of intelligence to support transformational needs and hybrid/multi-cloud adoption.

As organizations look to transform their business operations and revolutionize customer service, Digital Transformation (DX) is at the top of most CXOs' agendas; in fact, DX spending is expected to approach \$7.4 trillion between 2020 and 2023, a CAGR of 17.5%. However, according to the latest industry data released today from Veeam Software, the leader in Backup solutions that deliver Cloud Data Management, almost half of the global organizations are being hindered in their DX journeys due to unreliable, legacy technologies with 44% citing lack of IT skills or expertise as another barrier to success. Moreover, almost every company admitted to experiencing downtime, with 1 out of every 10 servers having unexpected outages each year — problems that last for hours and cost hundreds of thousands of dollars — and this points to an urgent need to modernize data protection and focus on business continuity to enable DX.

The Veeam 2020 Data Protection Trends Report surveyed more than 1,500 global

enterprises to understand their approach toward data protection and management today, and how they expect to be prepared for the IT challenges they face, including reacting to demand changes and interruptions in service, as well as more aspirational goals of IT modernization and DX.

“Technology is constantly moving forward, continually changing, and transforming how we do business — especially in these current times as we’re all working in new ways. Due to DX, it’s important to always look at the ever-changing IT landscape to see where businesses stand on their solutions, challenges and goals,” said Danny Allan, CTO and SVP of Product Strategy at Veeam.

“It’s great to see the global drive to embrace technology to deliver richer user experience, however, the Achilles Heel still seems to be how to protect and manage data across the hybrid cloud. Data protection must move beyond outdated legacy solutions to a higher state of intelligence and be able to anticipate needs and meet evolving demands. Based on our data, unless business leaders recognize that — and act on it — real transformation just won’t happen.”

The Criticality of Data Protection and Availability

Respondents stated that data delivered

through IT has become the heart and soul of most organizations, so it should not be a surprise how important “data protection” has become within IT teams, including not just backing up and restoring data, but also extending business capabilities. However, many organizations (40%) still rely on legacy systems to protect their data without fully appreciating the negative impact this can have on their business. The vast majority (95%) of organizations suffer unexpected outages and on average, an outage lasts 117 minutes (almost two hours).

Putting this into context, organizations consider 51% of their data as ‘High Priority’ versus ‘Normal’. An hour of downtime from a High Priority application is estimated to cost \$67,651, while this number is \$61,642 for a Normal application. With such a balance between High Priority and Normal in percentages and impact costs, it’s clear that “all data matters” and that downtime is intolerable anywhere within today’s environments.

“Data protection is more important than ever now to help organizations continue to meet their operational IT demands while also aspiring towards DX and IT modernization. Data is now spread across data centers and clouds through file shares, shared storage, and even SaaS-based platforms. Legacy tools

designed to back up on-premises file shares and applications cannot succeed in the hybrid/multi-cloud world and are costing companies time and resources while also putting their data at risk,” added Allan.

DX and the Cloud

Enterprises know they must continue to make progress with their IT modernization and DX initiatives in order to meet new industry challenges, and according to this report’s feedback, the most defining aspects of a modern data protection strategy all hinge upon utilization of various cloud-based capabilities: Organizations’ ability to do disaster recovery (DR) via a cloud service (54%), the ability to move workloads from on-premises to cloud follows (50%), and the ability to move workloads from one cloud to another (48%). Half of the businesses recognize that cloud has a pivotal part to play in today’s data protection strategy; and it will most likely become even more important in the future. For a truly modernized data protection plan, a company needs a comprehensive solution that supports cloud, virtual and physical data management for any application and any data across any cloud.

Allan concluded: “By already starting to modernize their infrastructures in 2020, organizations expect to continue their DX journey and increase their cloud use. Legacy solutions were intended to protect data in physical data centers in the past, but they’re so outdated and complex that they cost more money, time, resources and trouble than realized. Modern protection, such as Veeam’s Cloud Data Management solutions, go far beyond backup. Cloud Data Management provides a simple, flexible and reliable solution that saves costs and resources so they can be repurposed for future development. Data protection can no longer be tied to on-premises, physically-dedicated environments and companies must have flexible licensing options to easily move to a hybrid/multi-cloud environment.”

“Digital transformation is redefining the competitive business environment at an unprecedented rate. Anchored on key technologies like cloud, virtualization and modern storage systems, modernization of IT is critical to deliver business

continuity for rising customer expectations and de-risking business from evolving cyberattacks plus compliance measures. Our Veeam 2020 Data Protection Trends Report puts the spotlight on the importance of data management and protection across hybrid cloud environment. As the demands of a modern enterprise gets complex, it’s not enough for data to be backed up, data must in fact move to the higher state of intelligence and automatically anticipate demand, securely across physical, virtual and cloud environments. A simple, flexible and reliable Cloud Data Management solution is critical to build a robust foundation for today’s digital business”, said Mr. Sandeep Bhambure, Vice President & Managing Director, Veeam India & SAARC.

Other key highlights of the Veeam 2020 Data Protection Trends Report include:

The No. 1 challenge that will impact organizations within the next 12 months is cyber threats (32%). A shortage of skills to implement technology (30%) and meeting changing customer needs (29%) were also cited as key hurdles in the next 12 months.

Lack of staff to work on new initiatives (42%) was cited as the most impactful data protection challenge organizations currently have. Lack of budget for new initiatives (40%) and lack of visibility on operational performance (40%) were

also cited.

Over half (51%) of respondents believe DX can help their organization transform customer service. Almost half said it could transform business operations (48%) and deliver cost savings (47%).

Almost one-quarter (23%) of organizations describe their progress towards achieving DX initiatives and goals as mature or fully implemented.

Almost a third (30%) of organizations are currently in the early stages of implementing or planning DX.

Over a third (39%) of respondents said the ability to improve the reliability of backups is the most likely reason to drive their organization to change its primary backup solution. 38% cited reduced software or hardware costs and 33% said improving return on investment.

Almost a quarter (23%) of organizations’ data is replicated and made business continuity (BC)/DR capable via a cloud provider. Over a fifth, (21%) of data across organizations globally is not replicated or staged for BC/DR.

Over a quarter (27%) of organizations’ data is backed up to the cloud by a Backup as a Service (BaaS) provider. 14% of data across organizations globally is not backed up.

Over two in five (43%) organizations plan to leverage cloud-based backup managed by a BaaS provider within the next two years.



Half of the businesses recognize that cloud has a pivotal part to play in today’s data protection strategy; and it will most likely become even more important in the future.

For a truly modernized data protection plan, a company needs a comprehensive solution that supports cloud, virtual and physical data management for any application and any data across any cloud.

Cyber Actors use Online Dating sites to conduct Confidence/Romance Fraud & Recruit Money Mules



WHAT IS CONFIDENCE/ROMANCE FRAUD?

Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship—whether family, friendly, or romantic—and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor. In some cases, the victim is persuaded to launder money on behalf of the actor.

Actors often use online dating sites to pose as U.S. citizens located in a foreign country, U.S. military members deployed overseas, or U.S. business owners seeking assistance with lucrative investments.

THREAT - In 2017, more than 15,000 people filed complaints with the FBI's Internet Crime Complaint Center (IC3) alleging they were victims of confidence/romance fraud and reporting losses of more than \$211 million. In 2018, the number of victims filing these complaints increased to more than 18,000, with more than \$362 million in losses—an increase of more than 70 percent over the previous year.

In 2018, confidence/romance fraud was the seventh most commonly reported scam to the IC3 based on the number of complaints received, and the second-costliest scam in terms of victim loss.

IC3 receives victim reports from all age, education, and income brackets. However, the elderly, women, and those who have lost a spouse are often targeted.

METHODS - After establishing their victims' trust, scammers try to convince them to send money for airfare to visit, or claim they are in trouble and need money. Victims often send money because they believe they are in a romantic relationship.

For example, an actor claims to be a U.S. citizen living abroad. After a few months of building a relationship with the victim, the actor asks the victim to send gifts or electronics to a foreign address. After a few more months, the actor expresses a desire to return to the U.S. to meet the victim. The actor claims not to have the money to pay for travel and asks the victim to wire funds. In some cases, the actor claims the wired funds did not

arrive and asks the victim to resend the money. Some actors provide a fake travel itinerary. When they don't arrive as scheduled, they claim they were arrested, and ask for more money to post bail. They may also request more money for travel or to recover assets seized during their "arrest." Requests for money may continue until the victim is unable—or unwilling—to provide more.

TRENDS - In some situations the victim may be unknowingly recruited as a "money mule": someone who transfers money illegally on behalf of others. Actors groom their victims over time and convince them to open bank accounts under the guise of sending or receiving funds. Grooming is defined as preparing a victim to conduct fraudulent activity on their behalf through communications intended to develop a trust relationship. These accounts are used to facilitate criminal activities for a short period of time. If the account is flagged by the financial institution, it may be closed and the actor will either direct the victim to open a new account or begin grooming a new victim.

In other situations, the actor claims to be a European citizen or an American living abroad. After a few months of developing trust, the actor will tell the victim about a lucrative business opportunity. The actor will inform the victim there are investors willing to fund the project, but they need a U.S. bank account to receive funds. The victim is asked to open a bank account or register a limited liability company in the victim's name and then to receive and send money from that account to other accounts controlled by the actor.

TIPS TO PROTECT YOURSELF - Most cybercriminals do not use their own photographs; they use an image from another social media account as their own. A reverse image search can determine if a profile picture is being used elsewhere on the internet, and on which websites it was used. A search sometimes provides information that links the image with other scams or victims.

- ▶ To perform a reverse image search on profile photos:
- ▶ Right-click on the image and select "Search for an image."
- ▶ Right-click again and select "Save image as" to save the photo to your device.

- ▶ Using a search engine, choose the small camera icon to upload the saved image into the search engine.

Always use your best judgment. While most dating sites routinely monitor account activity and investigate all complaints of falsified accounts, most dating site administrators do not conduct criminal background checks when an account is registered. Keep in mind it is always possible for people to misrepresent themselves. Do not ignore any facts which seem inconsistent and be aware of the following common techniques used by romance scammers:

- ▶ Immediate requests to talk or chat on an email or messaging service outside of the dating site.
- ▶ Claims that your introduction was “destiny” or “fate,” especially early in communication.
- ▶ Claims to be from the U.S. but is currently living, working, or traveling abroad.
- ▶ Asks for money, goods, or any similar type of financial assistance, especially if you have never met in person.
- ▶ Asks for assistance with personal transactions (opening new bank accounts, depositing or transferring funds, shipping merchandise, etc.).
- ▶ Reports a sudden personal crisis and pressures you to provide financial assistance. Be especially wary if the demands become increasingly aggressive.
- ▶ Tells inconsistent or grandiose stories.
- ▶ Gives vague answers to specific questions.
- ▶ Claims to be recently widowed or claim to be a U.S. service member serving overseas.
- ▶ Disappears suddenly from the site then reappears under a different name using the same profile information.

The FBI advises:

- ▶ Never send money to someone you meet online, especially by wire transfer.
- ▶ Never provide credit card numbers or bank account information without verifying the recipient’s identity.
- ▶ Never share your Social Security number or other personally identifiable information that can be used to access your accounts with someone who does not need to know this information.

WHAT TO DO IF YOU ARE A VICTIM

- ▶ If you are a victim of a confidence/romance scam, the FBI recommends taking the following actions:
- ▶ Report the activity to the Internet Crime Complaint Center, your local FBI field office, or both. Contact IC3 at www.ic3.gov. Local FBI field offices can be found online at www.fbi.gov/contact-us/field.
- ▶ Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- ▶ Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.
- ▶ Report the activity to the website where the contact was first initiated.

Trend Micro Research Identifies Critical Industry 4.0 Attack Methods

For this report, Trend Micro Research worked with Politecnico di Milano in its Industry 4.0 lab, which houses real manufacturing equipment from industry leaders, to demonstrate how malicious threat actors can exploit existing features and security flaws in Industrial IoT (IIoT) environments for espionage of financial gain. “Past manufacturing cyber attacks have used traditional malware that can be stopped by regular network and endpoint protection. However, advanced attackers are likely to develop Operational Technology (OT) specific attacks designed to fly under the radar,” said Bill Malik, vice president of infrastructure strategies for Trend Micro. “As our research shows, there are multiple vectors now exposed to such threats, which could result in major financial and reputational damage for Industry 4.0 businesses. The answer is IIoT-specific security designed to root out sophisticated, targeted threats.”

“Politecnico di Milano is fully committed to supporting Industry 4.0 in addressing crucial aspects related to security and reliability of automated and advanced controls, especially as they gain relevance in all production sectors and increasingly impact business,” said Giacomo Tavola, Contract Professor in Design and Management of Production Systems and Stefano Zanero, Associate professor in Advanced Cybersecurity Topics for Politecnico di Milano.

Critical smart manufacturing equipment relies primarily on proprietary systems, however, these machines have the computing power of traditional IT systems. They are capable of much more than the purpose for which they are deployed, and attackers are able to exploit this power. The computers primarily use proprietary languages to communicate, but just like with IT threats, the languages can be used to input malicious code, traverse through the network, or steal confidential information without being detected.


Though smart manufacturing systems are designed and deployed to be isolated, this seclusion is eroding as IT and OT converge. Due to the intended separation, there is a significant amount of trust built into the systems and therefore very few integrity checks to keep malicious activity out.

The systems and machines that could be taken advantage of include the manufacturing execution system (MES), human-machine interfaces (HMI), and customizable IIoT devices.

The report offers a detailed set of defense and mitigation measures, including:

- ▶ Deep packet inspection that supports OT protocols to identify anomalous payloads at the network level
- ▶ Integrity checks run regularly on endpoints to identify any altered software components
- ▶ Code-signing on IIoT devices to include dependencies such as third-party libraries
- ▶ Risk analysis to extend beyond physical safety to automation software
- ▶ Full chain of trust for data and software in smart manufacturing environments
- ▶ Detection tools to recognize vulnerable/malicious logic for complex manufacturing machines
- ▶ Sandboxing and privilege separation for software on industrial machines

Use COVID-19 Downtime to Upskill for Digital

 Seven techniques to harness agile learning techniques to reskill and upskill employees for digital transformation.

Due to COVID-19 business shifts, one organization experienced an imbalance of resources across the company. With underutilized employees in customer service roles and overextended employees in remote service delivery, the executive team created an internal job board to match employees in slow parts of the business with experienced employees in other parts of the business that required more digital skills.

The experienced employee helped guide and train the newer employee, who was also offered a curriculum of on-demand training modules. Facing a similar challenge, another organization set up “ask an expert” forums to assist employees who were backfilling colleagues.

Both organizations accomplished two goals. They were able to shift employees to where they were most needed in the short term, but more importantly, the employees gained valuable and high-demand digital skills.

“Conditions during the COVID-19 crisis are harsh on learning and render traditional training nearly impossible,” says Graham Waller, Distinguished VP Analyst, Gartner. “Executive leaders can harness modern just-in-time remote microlearning to enable the upskilling opportunities they identify as supporting their COVID-19 recovery business objectives.”

How can organizations effectively future-proof employees, while also preparing for digital transformation? Be creative and be realistic.

Executives can focus on seven approaches for both upskilling and reskilling their current talent pool. Keep in mind when planning for learning opportunities that while some employees will have more downtime, others will be overwhelmed with family and home stresses, or — in certain industries and areas — stretched thin in their own job already. Take this into account when considering upskilling and reskilling plans.

1. Give employees explicit permission to learn

Employees will often hesitate to spend working time on training. This is normally considered secondary activity and is rarely prioritized by managers. Now employees are working from home with even more distractions like kids who are distance-learning or worries about at-risk family members.

Executives need to repeatedly and clearly state that it's okay to take time to learn new skills and that employees have explicit permission (and encouragement) to do so. Further, leaders should ensure that managers connect employees with opportunities to learn and set aside designated “development days” or scheduled times for training modules.

2. Take a learner-centric approach

Employees have a lot on their plates right now, which means executives must be extremely clear about the goals of each training module and ensure that employees who don't have time will not be penalized or pressured. For employees who do have extra time, frequent check-ins will ensure they understand how to prioritize learning with other tasks and can make continuous adjustments to align with business goals.

3. Emphasize on-demand consumable microlearning

If executives want employees to prioritize learning new skills, they need to make sure it's easy and convenient to do so. Focus on short, easy-to-digest learning content with optional deeper dives. Learning marketplaces can be a good option for organizations that are smaller or new to modern learning; many offer training for high-demand digital-era skills via free courses for a limited time.

4. Repurpose existing internal corporate training programs

This is a good time to rethink existing training programs for the current employee experience. For example, take longer courses and break them down into short, consumable bites. If your organization has relationships with external learning platforms like LinkedIn Learning, Degreed,

or Coursera, search for modules and learning pathways that focus on digital-era skills and highlight those for employees.

5. Blend content, coaching, and experiential learning

Experiential learning won't look quite the same in a remote context but find opportunities for pairing experienced employees with those less experienced. Take advantage of virtual platforms to schedule group training or have less-experienced employees shadow a mentor's meetings to observe them in action applying the skills.

Encourage employees with skill sets in high-demand areas to moderate a panel or lead a virtual module. Record all of these sessions to create a playback library for self-guided learning.

6. Cultivate learning communities of practice

Social learning, like chat boards or online interactive learning events, enables employees to share experiences and create a community in which they can support and teach each other. Highly skilled employees can help foster skills and offer practical help when most needed. For employees who are looking to develop digital skills, social learning offers a support system to gain confidence in new skills, which in turn helps the employee to deepen learning.

7. Embed microlearning in the flow of value

The goal should be to make reskilling and upskilling so easy the learner can consume it in their regular flow of work and immediately use it to help them achieve an outcome. This often means adding bite-sized (and highly relevant) learning opportunities into everyday meetings.

For example, a 5-minute learning video on how to make remote meetings more engaging should be added to regularly scheduled meetings and manager one-on-ones. For larger business priorities like cost optimization or setting up a remote service delivery capability, weave learning into the overall flow of the project meetings, and combine it with coaching from experienced employees.

WHERE YOU LEARN IS AS IMPORTANT AS WHAT YOU LEARN.



Dilsukhnagar Arena is the No.1 Centre of Arena Animation in India and the largest Training facility for **WEB, GRAPHICS, ANIMATION and VFX** in the country.

We ensure truly global standard facilities, world-class labs with Production-class technologies and finally the best placements. So, why join elsewhere?



© Creative Multimedia

Enhancing Employability™ of creative talent. Since 1998

📍 Arena Animation, Sai Towers, Main Road,
Dilsukhnagar, Hyderabad - 500036, Telangana.

📞 +91 801 901 3388
+91 801 901 3399

✉ enquiry@bestmultimedia.com

www.BestMultimedia.com

Extensive Industry Tie-ups | Regular Campus Drives | Revolutionary Initiatives | Multiple Value Additions

World Class GAMING STORE Now in Hyderabad



All Gaming Consoles, Games CD'S ,Accessories (Sale's & Service's). PS4 PRO, PS4 SLIM,PS4, XBOX ONE X XBOXONE S, PS3, XBOX 360, PS2,PS VITA, PSP ETC..



Published & Distributed by

World of Multimedia
COMPRINT

1st Floor, Pavani Kamal, Opp. SBH Gunfoundry,
Abids, Hyderabad. Ph - 040 66629647/48
e-mail : comprint@gmail.com
9248018430/31/34/36

For Demo Visit Us:



Watch on [youtube.com/comprintmultimedia](https://www.youtube.com/comprintmultimedia)



Be our fan on [facebook.com/comprintcdworld](https://www.facebook.com/comprintcdworld)



Be our fan on twitter.com/comprint



www.comprintcdworld.com



9154733845

*Conditions Apply