TECH & CAREER TOPICS - INSIDE

- SOPHOS Threat Report
- Password Security
- Credential Stuffing
- Smartphone Camera
- Data Breaches Report
- B2B Tech Startup Report
- 5 Security Mistakes
- WiFi 6 and 5G
- Gartner Reports & Many More .. Articles...

Threat Reports & Security Updates

Artificial Intelligence & Blockchain Updates

Six Best Practices for Password Security & TECH UPDATES
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

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
Be our fan on facebook.com/comprintcdworld
Be our fan on twitter.com/comprint
www.comprintcdworld.com
9154733845

*Conditions Apply
INSIDE BYTES

SOPHOS 2019 Threat Report .... 6
Password Security Tips .... 8
Credential Stuffing .... 10
Smartphone Cameras .... 12
2019 CEO Survey .... 16
Blockchain & Big Data ... 20
Blockchain as a Service .... 24
Wifi - 6 and 5G .... 26
Verizone Data Breaching ... 28
B2B Tech Startup Reports .... 30
5 Common Security Mistakes .... 32
Smartphones Report .. 33
Scammers target Job Seekers ... 34

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
Flexibility and Development Opportunities Are Critical to Appealing to the Digitally Native Employee.

A growing number of candidates are regretting their career decisions, according to Gartner, Inc. In 2018, 40% of Gen Z respondents reported that they would not repeat their decision to accept the job offer they had accepted and only 51% said they could see themselves having a long career at their organization.

Candidate regret leads to turnover, low engagement and low productivity; more than one-third of candidates who regret their decision intend to leave their position within 12 months. “To address this increase in candidate regret — and stem the ensuing issues with under performing talent and/or high turnover — organizations need to better understand what Generation Z candidates want,” said Lauren Smith, vice president of Gartner’s HR practice.

As digital natives, Gen Z candidates, those born from the mid-1990s to the early 2000s, understand that innovation and change are a constant. To ensure they are staying relevant as technology and business processes advance, Gen Z workers are keen to leverage various types of development opportunities, from training programs and boot camps to continuing education. Data from Gartner’s Global Labor Market Survey found that in 2018, 23% of Gen Z candidates listed development opportunities as a top attraction driver, compared with only 17% of their millennial predecessors in 2013.

Along with development opportunities, Gen Z candidates expect flexibility in their work arrangements. In addition to the ability to work from any location, these workers believe work should accommodate play and play should be incorporated in work.

"With this latest crop of workforce entrants, we are seeing an increased focus on work-life integration and the ability to pursue interests simultaneously both in and out of the workplace,” said Ms. Smith.

New Priorities

Compensation is no longer a guaranteed method for keeping the young workforce in seat, according to Gartner. In 2018, 38% of Generation Z candidates said that they would leave a job because of compensation, compared with 41% of millennials in 2013.

Gen Z candidates also differ from their millennial predecessors on seeking a defined career path. According to data from Gartner’s Global Labor Market Survey, in 2018, only 25% of Gen Z candidates listed future career opportunities as a top attraction driver when considering a job; in 2014, 34% of millennials felt the same way.

Managing Differently

“Given that today’s graduates are focused on learning and developing skills, employers looking to gain a career commitment from their Gen Z employees must ensure they offer these opportunities,” said Ms. Smith.

“Our research shows that more than anyone, it’s an employee’s manager who influences the type of development an employee gets on the job.”

In today’s digital age, graduates know they possess unique skill sets that are very much in demand and make up for a lack of experience. Management approaches must adapt to this new reality and shift from an “always-on” approach to a “Connector” manager approach.

Connector managers foster meaningful connections for their direct reports to and among employees, teams and the organization to develop an employee’s specific capabilities. Not only are managers crucial to ensuring their employees’ portfolio of skills stays relevant — a key concern of Gen Z — but they can improve the performance of employees by up to 26% and triple the likelihood that their direct reports will be high performers.

“Employers who want to capitalize on the influx of Gen Z candidates into the labor market must consider how best to appeal to these individuals and reduce the desire for them to seek alternative career opportunities,” said Ms. Smith.
OSMANIA UNIVERSITY, HYDERABAD - 7
Common Post Graduate Entrance Tests
CPGET - 2019

NOTIFICATION

Online Applications are invited from the candidates who have passed or appearing for the final year examination in the qualifying degree / Intermediate for entrance tests and admission into various P.G. Courses (M.A., M.Sc., M.Com, etc.), P.G. Diploma Courses and 5 yrs. Integrated Programmes (M.A., M.Sc., MBA) offered by Osmania, Kakatiya, Telangana, Mahatma Gandhi, Palamuru, Satavahana and Jawaharlal Nehru Technological Universities in their campus, constituent and affiliated colleges for the academic year 2019-20.

The Entrance test will be conducted online through Computer Based Test (CBT). For further details, go through the Information Brochure available in the websites:
www.ouadmissions.com or www.osmania.ac.in or http://tscpget.com

Registration Fee for a single subject is Rs.800/- for OC/BC candidates and Rs.600/- for SC/ST/PH candidates. For each additional subject, the fee is Rs.400/- for all categories. The fee may be paid at any TS/AP online centers or through payment gateway (Credit / Debit Cards / Net Banking). For submission of online application, visit the above websites.

IMPORTANT DATES

Date of commencement of online registration & submission of applications : 29.04.2019
Last date for submitting the online application : 30.05.2019
Last date with a late fee of Rs. 500/- : 08.06.2019
Last date with a late fee of Rs. 2000/- : 11.06.2019
Commencement of Entrance tests tentatively from : 14th to 26th of June, 2019

Prof. N. KISHAN
Convener, CPGET-2019

29.04.2019
Hyderabad
Sophos 2019 Threat Report unveils the rise of the hand-delivered, targeted cyberattacks as criminals stalk victims to bank millions.

Sophos launched its 2019 Threat Report providing insights into emerging and evolving cybersecurity trends. The report, produced by SophosLabs researchers, explores changes in the threat landscape over the past 12 months, uncovering trends and how they are expected to impact cybersecurity in 2019.

“The threat landscape is undoubtedly evolving; less skilled cyber criminals are being forced out of business, the fittest among them step up their game to survive and we’ll eventually be left with fewer, but smarter and stronger, adversaries. These new cybercriminals are effectively a cross-breed of the once esoteric, targeted attacker, and the pedestrian purveyor of off-the-shelf malware, using manual hacking techniques, not for espionage or sabotage, but to maintain their dishonorable income streams.” said Joe Levy, CTO, Sophos, as referenced in the SophosLabs 2019 Threat Report.

The SophosLabs 2019 Threat Report focuses on these key cybercriminal behaviours and attacks:

Capitalist cybercriminals are turning to targeted ransomware attacks that are premeditated and reaping millions of dollars in ransom – 2018 saw the advancement of hand-delivered, targeted ransomware attacks that are earning cybercriminals millions of dollars. These attacks are different than ‘spray and pray’ style attacks that are automatically distributed through millions of emails. Targeted ransomware is more damaging than if delivered from a bot, as human attackers can find and stake out victims, think laterally, trouble shoot to overcome roadblocks, and wipe out backups so the ransom must be paid. This “interactive attack style,” where adversaries manually maneuver through a network step-by-step, is now increasing in popularity. Sophos experts believe the financial success of SamSam, BitPaymer and Dharma to inspire copycat attacks and expect more happen in 2019.

Cybercriminals are using readily available Windows systems administration tools – This year’s report uncovers a shift in threat execution, as more mainstream attackers now employ Advanced Persistent Threat (APT) techniques to use readily available IT tools as their route to advance through a system and complete their mission – whether it’s to steal sensitive information off the server or drop ransomware:

Turning admin tools into cyberattack tools .. In an ironic twist, or Cyber Catch-22, cybercriminals are utilising essential or built-in Windows IT admin tools, including Powershell files and Windows Scripting executables, to deploy malware attacks on users.

Cybercriminals are playing Digital Dominos

By chaining together a sequence of different script types that execute an attack at the end of the event series, hackers can instigate a chain reaction before IT managers detect a threat is operational on the network, and once they break in it’s difficult to stop the payload from executing.

Cybercriminals have adopted newer Office exploits to lure in victims

Office exploits have long been an attack vector, but recently cybercriminals have cut loose old Office document exploits in favour of newer ones.

Eternal Blue becomes a key tool for cryptomining attacks

Patching updates appeared for this Windows threat more than a year ago, yet the EternalBlue exploit is still a favourite of cybercriminals; the coupling of EternalBlue to cryptomining software turned the activity from a nuisance hobby into a potentially lucrative criminal career. Lateral distribution on the corporate networks allowed the cryptojacker to quickly infect multiple machines, increasing payouts to the hacker and heavy costs to the user.

The continued threat of mobile and IoT malware – Malware’s impact extends beyond the organization’s infrastructure as we see the threat from mobile malware grow apace. With illegal Android apps on the increase, 2018 has seen an increased focus in malware being pushed to phones, tablets and other IoT devices.

As homes and businesses adopt more internet-connected devices, criminals have been devising new ways to hijack those devices to use as nodes in huge botnet attacks. In 2018, VPNFilter demonstrated the destructive power of weaponized malware that affects embedded systems and networked devices that have no obvious user interface. Elsewhere, Mirai Aidra, Wifatch, and Gafgyt delivered a range of automated attacks that hijacked networked devices to use as nodes in botnets to engage in distributed denial-of-service attacks, mine cryptocurrency and infiltrate networks.
SEE LIVE EVENTS
VIDEO Streaming

it’s easy...
its immediate.

See Live Events is a complete, full featured streaming service. It provides everything needed to broadcast live. The platform can be easy used to do high quality streaming and to monetize video as well.

- High Quality Live Video Streaming
- Ads free and no branding logos on player
- Wide Screen/Full screen/Cell phone apps support
- Embed player to your own websites
- Easy to use

“సమతల ప్రభుత్వ మంత్రి అనే మన జాతి వాల మనె నెహ్రూ వాల మనె నెహ్రూ వాల మనె నెహ్రూ వాల”

Flat.No.201, Vijetharama Enclave, Gouthamnagar, Dilsukhnagar, Hyd-60,
92 99 99 33 66 / 040-32 96 96 96
Fortinet, a global leader in broad, integrated and automated cybersecurity solutions, today reminded IT teams and stakeholders to maintain strong passwords and have a password strategy as an essential cybersecurity effort so that every employee and individual plays a crucial part in protecting corporate data.

According to the Verizon Data Breach Investigations Report, 81% of breaches leveraged either stolen and/or weak passwords. That problem is compounded because one of the biggest risks to data security is the reuse of passwords across accounts. If one of the accounts is compromised and your user name and password are posted on the dark web, cyber criminals who know how often passwords are reused will simply begin to plug that information into other possible accounts until they unlock one that uses the exact same credentials.

This is a common risk, as 83% of people have admitted to reusing passwords across multiple sites. Even if it is safe to reuse passwords on accounts that don’t house sensitive data – a breach there can be used as an entryway to move laterally across networks in search of critical business data or personally identifiable information (PII).

Rajesh Maurya, Regional Vice President, India & SAARC, Fortinet said, “Cyber adversaries are constantly tweaking their tradecraft to ensure successful intrusions in order to generate consistent revenue and profit. If your password is guessed or stolen, you may never know it happened until anomalous purchases appear in your bank account. And even more challenging data accessed by leveraging your compromised account may simply be used to move up the chain.” Implementing a strong passphrase is one of the easiest ways to protect yourself, your devices, personal and corporate data from cyber threats. The basic rule of thumb is, the longer and more complex the password, the more difficult it is to crack.

Short, simple passwords take fewer resources for hackers to compromise. In fact, hackers maintain databases of the most common words, phrases, and number combinations that they can run your password through to find a quick match. Some of the most common passwords are baseball and football team names, any variant of 123456789, and QWERTY. Avoid using common password themes when creating a passphrase, such as the following:

- Birthdays
- Phone numbers
- Names including movies and sports teams
- Simple obfuscation of a common word (“P@$$w0rd”)

The best password is a strong passphrase, impossible to forget and difficult to guess, even for someone who knows personal details of your life like the name of the street you live. When creating new accounts or updating well-used passwords.

Fortinet security experts recommend to keep these six best practices in mind to minimize password-based cyber risk:

1. Add an extra layer of security, use multi-factor authentication wherever possible. This confirms your identity by utilizing a combination of multiple different factors, such as something you know or something they have, such as a token generator on your smartphone.

2. Never repeat the same password for different accounts.

Change your passphrase at least every three months. This will lock out cyber criminals who may be using your account, protect you from brute force attacks, and remedy the issue caused by cyber criminals who purchase lists of usernames and passwords obtained through data breaches.

3. Ensure no one is watching as you enter passwords.

Be cautious when downloading files from the internet as they may contain key loggers as well as password grabber malware variants that will compromise your password. A good practice is to regularly scan for the presence of such malware.

4. Use a cloud-based password manager to enable you to create and store strong passphrases. This is especially important if you require strong passwords for dozens of accounts.

Password management tools allow you to securely store an encrypted list of passwords in the cloud that can be accessed from any device. Not only will you only need to remember one password to access your password locker, the passwords you store there for your various accounts can be even stronger because you don’t have to remember them.
Artificial Intelligence (AI) will affect one in every five jobs in Asia – eliminating one in eight, finds new report by MIT Technology Review Insights.

A new study by MIT Technology Review Insights in association with ADP, Infocomm Media Development Authority of Singapore, Genesys, Splunk and the Asia School of Business explores the degree to which executives in Asia Pacific are expecting and preparing for the automation of job roles. The report, “AI and human capital”, also examines how staff working in companies across the region are responding to the increasing need to work “shoulder to software.”

Featuring an executive survey of 900 leaders as well as a new data set provided by Faethm, a future-of-work cloud software company, the report shows, by country and industry, the proportion of formal sector jobs that will become redundant through automation, and the jobs that will be augmented by AI, making them more productive and highly skilled.

The findings are as follows:

Headcount reduction is not a major driver for AI in Asia. Corporate priorities for AI are to enhance customer satisfaction, decision-making, and reduce inefficiencies. It is likely this will lead to the loss of some roles to automation, and the restructuring of others. Yet reducing headcount is not in and of itself a top priority. Just one-third of survey respondents listed reducing labor costs as a top driver for AI.

The majority of companies are expecting headcount to increase. Some 77% of survey respondents expect total headcount to increase over the next five years, including in functions where AI is already being deployed. One fifth of respondents overall indicated that they expect five-year increases of more than 15%. Very few (just 3%) are predicting any headcount contraction.

Yet AI will affect one in five jobs in Asia—eliminating one in eight. Across 11 Asian markets, 12% of current jobs are at high risk of being automated in the next five years. The effect of AI on job automation will be greater in Asia’s wealthier economies than in poorer ones (14% as opposed to 10%). However, many more jobs in developed markets will actually benefit and be augmented by AI (11% of the total) than in less-developed markets (just 6%).

AI will produce winners and losers. In high-income countries, AI will result in significant job augmentation and added capacity, mostly in knowledge-intensive industries. In developing Asia, fewer jobs are augmented by technology, and little capacity is added. The impact is determined by the structure of each country’s economy, its technology-readiness, and other economic and social drivers.

“Our research shows that many industries across the region will see rapid automation and the loss of jobs,” says Claire Beatty, editor of the report. “In developed economies we’re likely to see re-skilling and redeployment. In developing markets, much more systematic planning and preparation is needed.”
Credential Stuffing: Another cyber-attack on the rise..!

by Naveen Joshi
Founder & CEO - Allerin, Mumbai

Credential Stuffing - another cyber-attack on the rise. Beware of an emerging security threat - credential stuffing - that involves bots making high-volume login attempts with stolen user credentials to execute catastrophic account hijacking and takeovers.

Credential stuffing attack forced Reddit to reset their user passwords. The company locked users’ account and implored them to reset their passwords and employ a two-way authentication security method. Just the beginning of 2019, and we see a cyber-attack already.

Hackers are hungrily waiting for customer data. We know this sad truth, yet most of us fail to follow a good Internet practice. Often we see warnings popping up while setting up a new account on any login page, which alerts us about the strength of the set passwords. Ignoring all the warnings, most of us still use the same credentials across multiple accounts or just enter the simplest password, say 123456. These poorly-crafted login credentials become one of the ways for malicious actors to execute their illegal activities. Let’s explore how:

What is credential stuffing?
When a data breach occurs, customer’s personal identifiable information is being compromised, which includes their login credentials also. Take the example of LinkedIn’s 2012 security incident. In the wake of this security breach, the company lost 167 million account credentials.

The spilled credentials are then used by hackers to execute their malicious agenda. They simply set an algorithm or design bots to test these breached credentials on a series of online applications. Due to the majority of reused and poor passwords, there is always a probability of 2 percent success rate for account takeovers.

Successful logins will enable hackers to carry out illicit activities, ranging from robbing credit card details to purchasing items of their choice to stealing medical data, and so much more. Not only customers but organizations also have to face major financial loss. According to Akamai’s report, “the total cost associated with credential stuffing, including fraud-related losses, operational security, application downtime, and customer churn can range from 6 million to 54 million dollars annually.”

How do businesses keep their customer login details safe? How would they know whether the login request is a legitimate one? As businesses fail to recognize the traffic coming in from a bad bot, they happen to give access to bad actors. Whom to blame? Is it organizations, who fail to distinguish a legitimate person from a software program, or is it customers who do not set strong and unique passwords? Well, actually both. But considering the organization’s angle, credential stuffing attack is so stealthy that it requires sophisticated tools to spot and guard against it. Fortunately, credential stuffing attacks are not carried out manually. This is probably one of the best chances to step in the battleground for defending against this attack.
How to mitigate credential stuffing attacks?

Over the past few years, hackers have evolved in carrying out malicious activities. Earlier, bots were programmed by simple scripts. These scripts were easily detectable by hunting down cookies. But as today’s sophisticated bots imitate the web browser, it becomes difficult for a bot management application to detect and distinguish between bad bots and good bots.

Similarly, credential stuffing attacks are difficult to detect. Organizations should, therefore, adopt advanced bot detection techniques like JavaScript challenge, device fingerprinting, and behavior-based detection systems.

**JavaScript challenge** – JavaScript codes are added to the HTML page of the browser. When the page is loaded, the JavaScript code also executes. The technique, JavaScript challenge is later used to detect if the traffic coming in is able to execute the JavaScript code. If the traffic is not able to execute the code, then it is considered as illegitimate. Such a technique solves the problem of sophisticated bots that emulates browsers.

**Browser/Device/machine fingerprinting** – Browser fingerprinting is one of the robust techniques that gather information about the browser. Every little information, right from its version to its type to active plugins to set language and font to other such characteristics is collected with the help of this method. A bot management solution will then easily monitor the browser fingerprint to detect malicious intent of the client. The solution can identify whether the client is actually a bot striving to trick an authorized browser.

**Behavior-based detection systems** – This is one of the most-sophisticated bad bot detection solutions. It accumulates and monitors customer inputs, behavior, and interactions, ranging from a mouse hover to keyboard strokes to site navigation to mouse clicks and so much more. This data is then fed to a bot management solution, which uses ML capabilities to identify a bad bot. For example, it is obvious that straight lines are difficult to be perfectly drawn with a mouse. Cases like this itself paints a story that the operator isn’t a human but a bot.
Today’s smartphone brands focus and harp more on ‘Camera’ capabilities than any other mobile features, when it comes to marketing. And, this strategy is not misplaced. CMR’s large-format Mobile Industry Consumer Insight (MICI) Surveys have confirmed that for Indian consumers, the brand preferences are increasingly being driven by camera specs, than, let’s say, smartphone brand reputation or associated brand imagery.

Given the importance associated with Smartphone camera, there is a steady and definite progress in terms of smartphone camera innovation. This is made possible by an unending competition between smartphone manufacturers to bring forth the best smartphone camera out there by replicating and replacing the professional camera. Whether it be more megapixels or the more lenses, or more cameras, or concepts such as pop-up or flip camera, the smartphone camera is going through its best phase of innovation.

Of late, smartphone brands such as Huawei and Nokia have been making waves with their strides in pushing photography forward.

Over the course of the past few years, smartphone brands have added more and more lenses to the primary camera. This, in turn, has given rise to concepts such as ‘dual’, ‘triple’ and even ‘penta’ camera lenses.

So, what role do the various types of smartphone lenses perform? And, what benefits do they bring in making the perfect picture possible?

**Wide angle lens**
A wide angle lens allows one to fit more into the frame, making them perfect for capturing scenes such as expansive landscapes or cramped interiors. Some flagship phones now feature wide angle lens, included the likes of Asus ROG phone, Asus Zenfone 5Z, Huawei Mate, iPhone Max, and LG V40 ThinQ.

**Telephoto lenses**
A telephoto lens is a type of camera lens designed for taking photographs of subjects at moderate to far distances. It allows the user to optimize the field of view to zoom in on an area of interest far away. The field of view on this type of lens is narrower than others. However, by using a telephoto lens with a second lens and a sensor, the phone camera can get one closer to the action.

Thanks to Telephoto lenses, one can get brilliant results on the portrait mode, whether it be through bokeh or focus effects.

Some of the dual-camera smart phones that have a telephoto lens, include Apple iPhone and, Samsung Galaxy Note 8, among others.

**Monochrome Sensor**
Monochrome sensor can capture greater sharpness and details as it passes all the color lights through the photo sites. As each photo site passes all the lights, more data are available to produce the image.

A few phones come with a secondary camera that is actually a monochrome one. These include smartphones from the likes of Huawei-Honor and Nokia.

During the past few months, there is a slow but steady hype cycle being built around something called a Time of Flight (or ToF for short) smartphone camera.

**Time of Flight (ToF)**
ToF is a camera sensor technology that uses infrared light to get depth information in a photo. The sensor emits a light signal, which is bounced back from the subject and returns to the sensor.

The ToF camera uses a technique known as range imaging to assist in taking a great photograph. In phones, TOF camera sensors will most likely be used for 3D photography, Augmented Reality (AR), and, in particular, Portrait mode. Thanks to the accurate depth information that ToF sensors develop, portrait mode photos can become more slicker, and the background blur can be done better.

Some recent smartphones, including the likes of Samsung Galaxy S10 5G, Huawei P30 Pro, and Oppo RX17 Pro, have the TOF feature.

Over the course of this year and in year ahead, smartphone camera innovation will continue to thrive. At the MWC 2019, Oppo unveiled its 10x Lossless Optical Zoom that one will be able to obtain from its new triple-lens cameraphone system. Similarly, Huawei’s latest Huawei P30 Pro also features a 5x periscope zoom. All said, the last word on smartphone camera innovation is yet to be written.
Digitization Emerging as the Key to Survival in Banking

Banks Must Increase Efficiency, Accelerate Processing, and Improve Decision Making to Revive Economic Profit; Raising the Bar on Regulatory Compliance Is Also Critical, Says New Report by BCG

With the momentum that has lifted the banking sector’s performance over the first half of the decade slowing in all major markets, banks must leverage digital technology to battle disruption and stem the threat of disintermediation brought on by fast-moving, newer entrants—or pay the price in staying power and profitability, according to a new report by Boston Consulting Group (BCG). The report, Global Risk 2019: Creating a More Digital, Resilient Bank, is being released recently.

This ninth annual survey of the health and performance of the banking industry by BCG examines global and regional profitability levels and how institutions can raise them, explores ongoing regulatory trends and how banks can navigate them, and examines how core risk and treasury functions must adapt both their operating models and their roles in the wider banking organization to be more efficient and effective.

“As digitization opens the financial services ecosystem to new and niche players, we expect to see fewer full-stack banks,” says Gerald Grasshoff, the global leader of BCG’s risk management segment and a coauthor of the report. “As the banking value chain breaks up, banks will get the opportunity to reposition themselves. They will likely pursue a mix of strategies, such as becoming platform leaders, being specialist providers, and promoting infrastructure-as-a-service offerings. The cost basis will also change, and banks will need to be leaner and more efficient if they are to compete effectively against digitally mature peers and fintechs.”

A Three-Speed World for Economic Profitability

According to the report, while banking remains profitable on an absolute basis, total economic profit (EP), which adjusts for risk and capital costs, softened again in 2017 (the last year for which year-end statistics are available). It was a second straight year of decline. Since reaching a global-average high of 16 basis points in 2015, EP has slumped, falling to just 8 basis points in 2017. With that slide, average banking performance is now on a par with that of 2013, when the banking industry started to regain its footing after the global recession.

In Europe, banks have remained mired in negative growth, hemmed in by low interest rates and nonperforming loans. By contrast, banks in North America have benefited from increasing interest rates, although rising costs edged total EP down for the second straight year. In Asia-Pacific, banks experi-enced the third consecutive year of declining EP. Overall, banking remains a three-speed world in which European banks continue to struggle, North American and Asia-Pacific banks strive to stay the course, and the developing markets of South America and the Middle East and Africa continue to show high profitability. Yet system-ic issues hound each region.

Setting the Regulatory Stage for the Future of Banking

The report says that, for regulators, instilling trust in the strength and resiliency of financial markets has become a dominant focus. Banks must improve the quality and efficiency of regulatory compliance to meet their ongoing financial-stability, prudent-operations, and resolution obligations. Achieving this will require finding leaner and smarter ways to manage the high volume of regulatory revisions, as well as experimenting with new technologies and partnerships to drive down the cost of know-your-customer documentation and to improve anti-money-laundering processes.

Keen to protect financial markets from future shocks, regulators are trying to anticipate the ways that technology will reshape the banking ecosystem and, with it, their own role in establishing guidance and ensuring consistent standards. Moreover, since 2009, banks worldwide have paid $372 billion in penalties. Regulators assessed $27 billion in penalties on European and North American banks in 2018, an increase of $5 billion from the year before. Mortgage-related misconduct in the US, money laundering and interbank-offered-rate-related market manipulation across regions are among the factors sparking regulatory ire.

As Banks Digitize, So Must Risk and Treasury...

The report says that banks’ risk and treasury functions will change in profound ways over the coming years. Both functions face a broader mandate with a larger slate of risks to manage, a growing need for integrated steering to protect banks’ interests, and an equally growing need to make the most strategic use of banks’ balance sheet resources. Delivering on this mandate will require risk and treasury to operate faster and more incisively, backed by real-time data, predic-tive analytics, and end-to-end automation. Risk and treasury functions that commit to “going digital” in these ways will become not only more efficient operators but also more effective strategic partners in delivering value to banks.
Globally, the feature phone segment is forecast to generate around US$16 billion cumulatively in wholesale hardware revenues over the next three years. India remains the largest market in terms of potential feature phone volumes followed by Bangladesh and Nigeria.

In contrast to the smartphone market, which contracted for the first time in 2018, the feature phone market has continued to grow over the last three years. Latest research from Counterpoint Research estimates that in 2019, a little more than 400 million feature phones will be sold globally. Further, feature phone shipments are expected to cross one billion units by 2021.

According to Peter Richardson, Research Director at Counterpoint Research, India and the Middle East Africa region will drive the growth of the global feature phone market by capturing nearly three-quarter of the market share in 2019. “India and the Middle East Africa region will see cumulative shipments of around 800 million feature phones out of more than one billion global feature phone shipments over the next three years. Globally, the feature phone segment is forecast to generate around US$16 billion cumulatively in wholesale hardware revenues over the next three years,” Peter says.

While India remains the largest market in terms of feature phone volumes, it is closely followed by Bangladesh and Nigeria. In Africa, growth is led by brands like itel and TECNO. Much of the growth of feature phones in India has been driven by the revival of the Nokia-branded features phones and the popularity of the Jio Phone, a smart feature phone which packs a chipset and an operating system that can support sophisticated smartphone-like features in a traditional feature phone form-factor. The Jio Phone uses KaiOS as the operating system. KaiOS has also been expanding its reach in Africa. At the recently held Mobile World Congress in Barcelona, KaiOS announced partnerships with African operator Orange to launch KaiOS-powered smart feature phones priced at US$20 across 16 countries in Africa and the Middle East.

There are several reasons why feature phones are the preferred mobile phone in many markets globally, despite the tremendous adoption of smartphones. An important factor is affordability. The bottom of the pyramid population across the world simply cannot afford a smartphone.

“There are more than three billion people across the world who live on an income of less than US$2.50 per day. This segment can neither afford a smartphone nor the data services demanded by the growing advancement in smartphone use-cases. Thus, a feature phone, coupled with basic mobile services has been the go-to offering for these users to communicate and connect. Most of these users are prevalent across Africa, parts of Asia and Latin America,” says Tarun Pathak, Associate Director at Counterpoint Research.

There is also a business case for network operators to push feature phones. In most markets, network operators want customers to upgrade from 2G/3G to 4G networks. “The problem is most of these users still cannot afford a 4G smartphone. Therefore, operators and the mobile industry players need to offer 4G VoLTE feature phones and move users to the more efficient 4G network,” says Pathak.

Counterpoint Research believes the rise of 4G capability in feature phones will be one of the key trends moving forward which will allow the feature phone segment to remain relatively resilient in the medium term.

Further, there are also several use cases that are driving the sales of feature phones. For example, industry segments like construction require rugged devices with technologies like PTT (Push-To-Talk) to cope with the hostile environment. Feature phones offer a viable alternative for this segment.

Similarly, there is also a need for longer battery life. Varun Mishra, Research Analyst at Counterpoint Research explains, “The emerging markets of India and Nigeria have the greatest number of people without access to electricity. Amid the dearth of electricity, in some cases, the user is dependent on public charging stations (shops giving facilities to charge phones in return for a payment). Long battery life becomes crucial in such situations.”
Synopsys Report Finds that Open Source Risk Management is Improving

Synopsys, Inc. recently released the 2019 Open Source Security and Risk Analysis (OSSRA) report. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of more than 1,200 audits of commercial applications and libraries, performed by the Black Duck Audit Services team. The report highlights trends and patterns in open source use, as well as the prevalence of both insecure open source components and license conflicts.

As shown in the report, many of the trends in open source use that have presented risk management challenges to organizations in previous years persist today. However, the data also suggest that an inflection point has been reached, with many organizations improving their ability to manage open source risk, possibly due to heightened awareness and the maturation of commercial software composition analysis solutions.

"Open source plays an increasingly vital role in modern software development and deployment, but to realize its value organizations need to understand and manage how it impacts their risk posture from a security and license compliance perspective," said Tim Mackey, principal security strategist of the Synopsys Cybersecurity Research Center. "The 2019 OSSRA report provides a glimpse into the state of open source risk management within commercial applications. It shows that there are still significant challenges, with the majority of applications containing open source security vulnerabilities and license conflicts. But it also highlights that these challenges can be addressed, as the number open source vulnerabilities and license conflicts have declined from the previous year."

Some of the most noteworthy open source risk trends identified in the 2019 OSSRA report include:

- There has been a significant uptick in open source adoption. Ninety-six percent of codebases audited in 2018 contained open source components, with an average of 298 open source components per codebase compared to 257 in 2017.

- Open source license conflicts can put intellectual property at risk. Sixty-eight percent of codebases contained some form of open source license conflict, and 38% contained open source components with no identifiable license.

- The use of ‘abandoned’ components is common. Eighty-five percent of codebases contained components that were more than four years out-of-date or had no development in the past two years. If a component is inactive and no one is maintaining it, that means no one is addressing its potential vulnerabilities.

- Many organizations are failing to patch or update their open source components. The average age of vulnerabilities identified in 2018 Black Duck Audits was 6.6 years, slightly higher than 2017—suggesting remediation efforts haven’t improved significantly. Forty-three percent of the codebases scanned in 2018 contained vulnerabilities over 10 years old. When viewed against the backdrop of the National Vulnerability Database adding over 16,500 new vulnerabilities in 2018, its clear patch processes need to scale to accommodate increased disclosures.

- Not all vulnerabilities are created equal, but many organizations aren’t even addressing the riskiest ones. Over 40% of codebases contained at least one high-risk open source vulnerability.

The report notes that the use of open source software is not a problem in and of itself, and is, in fact, essential to software innovation. But failing to proactively identify and manage any security and license risks associated with the usage of open source components can be very damaging. Despite the risk factors identified, the 2019 OSSRA data suggests that, in the wake of the Equifax breach, an increase in awareness of open source risk and the maturation of commercial software composition analysis solutions has led to forward progress:

- Organizations are getting better at managing open source security vulnerabilities. Sixty percent of the codebases audited in 2018 contained at least one vulnerability—still significant, but much better than the figure of 78% from 2017.

- Overall, open source license compliance has improved as well. Sixty-eight percent of the 2018 audited codebases contained components with license conflicts, compared to 74% in 2017.
Why CIOs should focus on diversification, executive education and geographic opportunities in 2019.

In late 2018, a CEO called together her leadership team to discuss strategies and focuses for the upcoming year. Although she had been focusing on opportunities for deeper, more structural growth, her strategy now is diversifying the organization and getting everyone on board with a digital business model. And she’s counting on the CIO to help. “CIOs must apply technology to help CEOs diversify revenue streams, sustain profitability and support key geographic moves in a waning global economic cycle,” says Mark Raskino, Distinguished VP Analyst, Gartner.

“CEOs need CIOs to be more than service-oriented order takers. They expect IT leaders to work with business leaders to co-develop technology-related capabilities,”

The Gartner 2019 CEO Survey looked at responses from 473 business leaders from 32 countries. The leaders ranked simple growth, IT-related items, corporate (structural development), financial, workforce and customer as top strategic business priorities for 2019 and 2020.

Mentions of simple growth (grow revenue, increase sales, expand market share) increased, while mentions of structural development (change strategy, mergers and acquisitions, and company reorganizations) fell, reversing the trend from 2018. Additionally, CEOs mentioning “digital” within their top five strategic business priorities rose to include 20% of all surveyed.

**Focus on diversification to increase growth**

With weakening profit margins and softening growth prospects, CEOs are looking for new areas of revenue. Mentions of diversification were five times higher than in last year’s survey. The most effective options for diversification will depend on the industry and organization. For a retail company, the focus could be adding a few more products. For some organizations, purchasing a company in an adjacent industry will offer the best value. CIOs should also consider how upselling or cross-selling might add additional revenue-producing channels to the mix. Some CIOs should help to create new digital products and services.

**Leverage geographic changes**

When asked where CEOs will look for opportunities in the face of slow growth, the most popular solution was to literally look elsewhere. Mentions of other states, cities, countries and regions — as well as “new markets” — highlight a focus on location hunting for growth when traditional or home markets lack opportunity. This is a chance for CIOs to integrate digital initiatives and blend them into the new facilities, locations, suppliers and markets. New geographic locations can also offer opportunities to test out new ideas without the competition or pressure the organization would face in the home market.

**Highlight technology opportunities for growth**

CEOs need CIOs to be more than service-oriented order takers. They expect IT leaders to work with business leaders to co-develop technology-related capabilities that will enable the business to innovate and grow. In fact, 49% of CEOs believe business and technology have an equal responsibility for the performance and quality of digital products and services.

This is an opportunity for CIOs to explore and advocate for technology that would increase productivity, and showcase how technology would allow the organization to lean into any economic downturn. This is particularly important given that 27% of
CEOs ranked technology enablement as third in ways that organizations will exert cost controls. But 47% ranked technology enablement as one of their top two ways to improve productivity.

**Elevate the executive committee**

CEOs want to grow digital and are increasingly impatient with limited returns on large investments. The number of CEOs agreeing they had a management initiative or transformation program underway to make the company more digital rose to 62% this year, despite challenges with technology and cybersecurity concerns. However, very few organizations have made major changes in business models to support this new change or transformation.

“Digital requires each executive to be on board, because digital products are complex and across the company”

Part of the issue is that the executive team will not all have equal amounts of digital business acumen, yet digital is a team sport. Without confident involvement of the entire executive team, it’s difficult to enact real change. Each member of the executive committee needs to be fully engaged, understand their role in the transformation and feel confident in execution.

Digital requires each executive to be on board, because digital products are complex and across the company. For example, Nike developed and marketed a shoe that fastens itself via mobile app and collects data via sensors to send back to the company. General Motors and Volvo developed and delivered the ability to have Amazon deliver packages to car trunks using a one-time digital key to unlock the trunk wirelessly. These complex, multifaceted endeavors require all the functions of a company.

### Three out of Four Smartphones Forecast to Have Dedicated AI Processors by End of 2022

![Three out of Four Smartphones Forecast to Have Dedicated AI Processors by End of 2022](image)

Dedicated processors will dramatically expand the use of AI in smartphones with voice assistants being one of the first beneficiaries of ‘on-device’ AI processing. Smartphones have been leveraging the capabilities of artificial intelligence (AI) for some time. However, till now the processing has been done either in the cloud or distributed across the various computer chips in the device such as CPUs, GPUs, and DSPs.

As AI becomes part of the mobile experience, smartphone system-on-chip (SoC) vendors are racing to improve the machine learning capabilities of their chips by integrating dedicated AI processing cores into their designs. The key benefits of this are higher AI processing performance and lower power consumption. However, this must be balanced against the actual need for AI processing, which until recently has been limited.

At present, AI is being used mostly for camera-related applications (facial recognition, image enhancement, and more). However, Counterpoint Research expects to see AI being used extensively for a raft of other applications over the next two years.

“We see voice assistants as one of the first applications to benefit from device-based processing,” said Gareth Owen, Associate Research Director at Counterpoint Research. “Today, most voice processing in smartphones is cloud-based. However, voice assistants will be able to process commands quicker and respond faster with on-device processing. It also resolves privacy concerns,” he added.

Apple and Huawei were the first OEMs to include dedicated AI processors in their SoCs (A11 and Kirin 970 chips respectively) launched in their flagship handsets in September 2017. Two years on, virtually all other SoC vendors are following suit. For example, Qualcomm is offering an AI Tensor Accelerator in the Snapdragon 855’s Hexagon DSP for the first time.

Counterpoint Research forecasts sales of AI smartphones will increase to 1,250 million units in 2022 from 190 million in 2018, representing more than three-quarters of all smartphones shipping in that year.

A key driver behind this forecast is the expected launch of several Android smartphone models using Qualcomm’s 855 SoC in 2019 and beyond. Counterpoint expects that dedicated AI cores will also be included in some mid-range smartphones during 2019 using Taiwanese vendor MediaTek’s new P90 SoC.

Although AI may not be immediately visible to smartphone users today, as the machine learning market evolves and more applications appear, smartphones with dedicated AI hardware will clearly be at an advantage.

“With Qualcomm joining the fray and incorporating hardware-based AI acceleration in its latest Snapdragon SoC for the first time, industry-wide adoption of AI silicon in smartphones is inevitable,” said Peter Richardson, Research Director at Counterpoint Research. “And with Qualcomm keen to extend machine learning capabilities into its lower cost chips, plus the availability of AI SoCs for mid-range phones from other vendors, this trend will quickly extend to mid-range and even low-range smartphones,” he added.
Over 1500 professionals across the globe to attend

Latest trends in HR, Technology, and Workplace Innovation to be discussed

SHRM Hackathon, to create tech solutions for real-world workplace problems

Technological disruption and automation are transforming the Work, Worker, and Workplace. Whether it's a large multi-national company or a small to mid-sized business, the HR systems and organizational processes should respond to the changing world of work. With a never-ending march of technological development, varying levels of digital maturity, complex organizational needs and differing approaches to adoption, it is essential that HR professionals keep up-to-date with the latest business tools, strategies, and insights available.

It's all in the spotlight at SHRM HR Tech APAC Conference 2019, essential event connecting C-suite and senior decision makers across HR to cut through the jargon and explore how organizations are approaching this constant change, providing analysis of the latest in HR technology and the impact it has on business strategy. The theme will throw the spotlight on creating digital workspaces, integrating workforce with technology and addressing challenges that organizations face in adopting technology in its entirety.

Featured in 20 Best HR Conferences to attend in 2019 by Harver, SHRM HR Tech APAC 2019 will be the most powerful confluence of people, business and technology. The conference happening at Hyderabad International Convention Center (HiCC), Hyderabad on 22nd and 23rd May 2019, will see an attendance of over 1500 professionals from the world of work and bring them closer to expert opinions, global leaders and latest trends in HR, Technology and Workplace Innovation.

Some of the esteemed speakers for the conference this year are Sharad Sharma, Co-Founder, ISPIRT Foundation; Suresh Kumar Sethi, Managing Director & CEO, India Post Payments Bank; DR. Shawn G. Dubravac, Founder & President, Avrio Institute; Shri. Jayesh Ranjan, Secretary, Information Technology (IT) Govt. Of Telangana; Suresh Narayanan, Chairman & MD, Nestle India Limited; Emily M. Dickens, J.D Corporate Secretary & Chief Of Staff, SHRM; Raj Raghavan, Senior VP, HR at Indigo.

Announcing the conference, Ms. Achal Khanna, CEO – SHRM India and Business head- MENA & APAC, quoted, “We are once again back with SHRM HR Tech APAC 2019, the biggest platform for the HR & Tech experts across the globe to gather, network and discuss the technological disruptions at the workplace. Our last four conferences were huge success in terms of high quality relevant delegation, highly engaged knowledge sessions, electrifying keynotes and much more. We are hopeful that this year too we would be able to meet the expectations of our delegates and make the conference a huge success”.

SHRM India is coming up with SHRM Hackathon, an initiative aimed at building a hub for fostering innovation and nurturing new ideas and budding tech talent. This Hackathon, spearheaded by SHRM India along with its partners, helps handpick the best WorkTech innovators and showcase them at SHRM HR Tech APAC 2019 – bringing together the startup ecosystem enablers such as noted investors, government officials, academia, influencers, mentors, media, and startups. Organizations are in constant need for new ideas, better solutions to maximize user experience at the lowest possible cost. Maybe this is one of the reasons that the HR Tech Market in India is pegged at between $600-700 million! There are solution-providers out there for all business challenges and needs. But, with a myriad of options available, the ones with true potential sometimes go unnoticed. To provide such start-ups, small business a recognizable platform and foster innovation, SHRM India has launched a special Start-up initiative, SHRM APAC Start-up Network.
The Indian ecommerce sector is bracing itself for a summer launch by Jio. Jio has plans to launch the world’s largest Online-to-Offline (O2O) e-commerce platform. Alongside, it is also investing its energies in creating a ‘Super App’, imagine a broad digital ecosystem that will provide over 100 services at one go. Previously, many companies, including Flipkart and Paytm, have aspired to create a super app in India, but have been unable to breakthrough.

The Pioneering Super App : WeChat

The genesis of the ‘Super App’ can be traced to China’s successful WeChat, that counts over a billion active users globally. Known in China as Weixin, the local WeChat version enables one to send and receive money, shop online, order food, pay utility bills, or even, check-in on flights. Broadly speaking, WeChat can be bucketized into social media, information via blogs, ecommerce and utility payments, and ‘mini programs’ that offer games, access to offline events, discounts and much more. In essence, WeChat is a one-stop ecosystem that offers all the functionalities that the likes of Whatsapp, Facebook, Amazon, Uber, Apple Pay and others offer on their individual apps. Why is WeChat successful? Launched in 2011, WeChat quickly captured a market of mobile-first, digital explorers, by offering a bouquet of services. And, over a period of time, WeChat has evolved itself, and dominating the landscape.

Jio and the Indian Super App

Just like China, India is a mobile-first nation. Many Indians have found true independence via their mobiles. Whether it be economic progress or education, access to healthcare, or consuming entertainment, the mobiles have played a key role in shaping new realities for Indians everywhere.

Interestingly, 4G devices shipments grew to 215 million at end-2018, from a mere 75 million two years ago. This growth can be traced to the entry of Reliance Jio in the telecom sector.

The ubiquitousness of Jio devices has given Reliance Jio a broad platform to segway into ecommerce. Reliance Jio can tap into, and connect its vast ecosystem of its users via a multi-layered fabric. Such a fabric can offer a rich array of services, in an online-to-offline ecommerce model, and facilitated through a one-stop, super app. Such a self-contained network that offers convenience will find favour with Jio’s consumer base.

Jio’s ‘Super App’ Tech Stack

Over the past many months, Jio has been actively pursuing a proactive strategy of tech acquisitions and investments. As a result, the tech stack at Reliance Jio now includes a Conversational AI layer, a vernacular layer, a logistics layer, a content layer, as well as a AI-based education layer. All of these layers, on top of the Jio devices network potentially puts Reliance in a pole position to create India’s WeChat, where others failed.

A String of Acquisitions

Almost a year ago, Reliance Jio kicked-off its aggressive strategy. It integrated JioMusic, and Audio OTT platform, Saavn. JioSaavn, the combined entity, competes against the likes of Amazon Music, Apple Music, and Gaana. A month later, Reliance invested in Embibe, an AI-based education platform. Jio followed-up by picking-up a majority stake in Den Networks and Hathway Cable and Datacom.

Its most recent acquisition, Reverie Language Technologies builds language technologies to offer a language-as-a-service model. Reliance also acquired the acquisition of logistics services platform Grab-a-Grub. In March 2019, Reliance announced the acquisition of ConversationalAI company, Haplik. In the coming months, Jio is also readying to launch Jio GigaFiber and GigaTV services.

Over the coming months, Reliance Jio will step-up on their aggressive acquisition strategy. Jio’s O2O ecosystem will encompass a vast network of 12 million kirana stores nationwide. In addition, Reliance Retail plans to convert >5000 Jio point of sales stores, across 5000 cities and towns, into delivery and collection points.

Jio’s user base in rural India posits a vast unexplored, and untapped ecommerce market opportunity. If Reliance ensures that the last-mile delivery is seamless, it will have the tailwinds to carve out a niche for itself in India’s ecommerce sector.

Imagine such a vast user base, using the JioApp, conversing in their local language, consuming content, communicating, and most importantly, transacting online using just VoiceAI.
Multiple organizations can monetize their data to increase their revenue. In data monetization, blockchain can be a major contributor due to its advanced applications and decentralized nature.

The fourth industrial revolution has led to the rise of data-driven business models. Organizations collect large volumes of data from every department using modern technologies such as big data and IoT. Every organization has realized that data is an asset and utilizes crucial data in multiple applications. However, numerous start-ups and small businesses don’t have access to infrastructure and resources for collecting and analyzing crucial data. To address this issue, well-established organizations can implement data monetization to sell relevant data to upcoming businesses. With this approach, data sellers can generate new revenue streams for their business.

Several sources suggest that data monetization is a necessity for businesses. Using data monetization, multiple organizations can help create a marketplace for sharing critical data. Such marketplaces can democratize the collection and analysis of data. Hence, small and medium businesses and startups can easily tackle the cold start problem. Besides, big players can also benefit from data monetization as their data collection and analysis tasks will be simplified while expanding their business in different sectors.

**How can organizations collect and analyze data?**

To speed up collection and analysis of data, organizations can deploy modern technologies such as big data and IoT. Such technologies can help collect and analyze data in the following manner:

**Big Data**: Every online activity and business procedure generates a large volume of data. Organizations can collect various types of historical and real-time data like customer data, social media data, employee data, and operational data. Businesses can analyze such data to draw insights into their customer demographics, employee performance, and business operations. Big data can process large volumes of data at a great velocity to generate accurate results. Hence, big data can be utilized across various industry sectors such as healthcare, retail, finance, manufacturing, and many more. For instance, in retail, organizations can collect customer details and social media feedback to generate personalized marketing campaigns for specific customer demographics.

With the help of big data, organizations can analyze large data sets from different sources to generate complex data models. Using these data models, business leaders can predict upcoming market trends and develop strategies for adapting to these trends. Such strategies include actionable steps to address inventory requirements, production, marketing, and sales. Also, organizations utilize big data analytics to make decisions about product launch and pricing.

**IoT (Internet of Things)**

Several organizations and smart cities have deployed IoT devices for multiple applications. For example, manufacturing organizations can install IoT sensors to monitor production flow, from the refining process to final procedures such as packaging, in real-time. Such advanced applications have led to the increasing adoption of IoT devices. In addition to big data, organizations can utilize IoT data for more accurate results. Analysis of such data helps organizations measure and understand various business procedures. For example, in retail stores, IoT sensors can be installed in shelves to notify the store owner when products are running out. The sensors can collect data that can help the store owner understand which product is in high demand, at what time the shelves go empty, and which days customers buy the most products. Using such insights, the store owner can make key decisions about inventory management, product orders, and discounts.
How can organizations implement data monetization?

To implement data monetization and increase revenue, business leaders need to create an effective strategy. Business leaders can consider the following steps in their strategy:

Recognize different types of data and their use cases
Organizations can collect various types of data from different sources such as social media, IoT devices, cloud, and the web. Every organization specializes in collecting specific types of data. For instance, healthcare organizations collect data regarding patients, doctors, disorders, treatments, medicines, and hospitals. To sum up, business leaders have to ask important questions such as:

What type of data does the organization gather?

What kind of insights can be drawn from the collected data?
With the help of such questions, business leaders can identify innovative use cases for the collected data. Using the above example, data collected by healthcare organizations can be used by pharmaceutical companies to understand which medicines are in demand and plan for the production and inventory requirements. Business leaders have to identify all possible use cases of their data to maximize their data monetization revenue. Also, organizations need to ensure that they are sharing anonymized data to avoid privacy violations.

Identify prospective buyers
After recognizing all possible use cases for accumulated data, organizations have to segment their collected data based on various use cases. Based on the use cases, organizations can identify prospective buyers for their data. These buyers can be start-ups or other well-established organizations. For instance, retailers gather extensive customer data that can be beneficial for other organizations in the manufacturing sector for use cases like improving product quality by analyzing customer demographics and their purchase patterns.

Interested buyers can also be big players that are planning to expand their business into different sectors. Such organizations may want to simplify data collection and analysis tasks and focus more on mergers and acquisitions in their target market. For example, if an electronics manufacturer is planning to enter the telecom market, then the organization may buy critical data from a telecom company to speed up their expansion. Hence, organizations need to be mindful about use cases of their data and how the data can benefit multiple organizations. Once business leaders have identified their prospective buyers, they have a key decision to make. Business leaders have to decide whether they would sell data via a blockchain-based data monetization company or independently.

Select a suitable blockchain-based data monetization company
Blockchain has the potential to democratize data monetization and sharing. Looking at this potential, several entrepreneurs established blockchain companies that specialize in data monetization. These companies enable organizations to buy and sell data collected using IoT sensors, big data, and VR/AR. Hence, business leaders have to identify what type of data they can provide. To select the most suitable blockchain-based data monetization company, business leaders need to research various companies, the type of data they monetize, the services they offer, and their costs. After finding the most appropriate blockchain-based data monetization firms, business leaders can decide which company they want to do business with, based on their budget.

Implement data monetization independently
Organizations can also monetize their data independently. For this purpose, business leaders need to hire professionals with niche skills. Then, organizations must adopt blockchain networks for data exchange and storage. Decentralized blockchain networks will record every instance of data exchange and encrypt all the data. For blockchain-based storage, organizations can deploy various secure blockchain wallets. Organizations can store different types of data from several sources in different wallets to segregate large volumes of data. Such blockchain wallets are encrypted and employ a secure authentication mechanism to restrict data access.

Using these wallets, organizations can share data with prospective buyers. Also, organizations can utilize smart contracts to verify the credentials and documents of their buyers, receive payments, and automatically share relevant data. With this approach, organizations can implement an autonomous data monetization process.

With the help of blockchain, data monetization will be accessible to consumers soon.

Using blockchain-based data monetization, consumers can monetize and negotiate the value of their data. Also, consumers can control which data can be collected by organizations to ensure data security and privacy.

How can organizations implement data monetization?

Recognize different types of data and their use cases
Business leaders have to understand which types of data their organization collects from different sources and identify all possible use cases of the collected data.

Identify prospective buyers
Organizations need to identify startups and other organizations that might be interested in buying data.
According to a BCG Study, AI Will Create New Efficiencies for Biopharma, Providers, Payers, and Medtech Companies – But It Is Also Likely to Cause Some Value to Flow to Technology Players and Consumers

Companies in the four traditional sectors of health care risk ceding much of the value created by AI tools to technology players and consumers, according to a new publication by Boston Consulting Group (BCG). Although AI will create significant efficiencies for biopharma companies, providers, payers, and medtech companies, those traditional players may not retain a sizable portion of the value created. The article, titled Chasing Value as AI Transforms Health Care, is being released today.

The article assesses two possible scenarios for the value pool shifts created by AI. Under the first scenario, players in all four traditional sectors retain the value unlocked by improvements in their own efficiency. At the same time, medtech, providers, payers, and non-traditional health care companies from the technology sector capture much of the additional value created by AI—while the impact on biopharma is likely neutral. Under the second scenario, consumers benefit significantly.

Artificial intelligence is to some degree already being deployed across all incumbent sectors of health care today and will play an exponentially larger role in the years ahead,” says BCG Partner Alexander Aboshiha, coauthor of the article. “Companies need to move quickly to harness this rapidly developing technology—including by ensuring they have access to the right data and the right talent to succeed.”

Health Care Players Are Making Major AI Investments

The article also outlines areas within health care for which AI spending will total $8 billion by 2022. These include:

- **Remote Prevention and Care**: AI can be used to serve patients outside their doctor's office or the local hospital. Virtual agents, for example, can conduct an initial consultation with a patient, screening out those who do not need to see a doctor and providing important information to physicians about those who do need treatment. Wearables or other devices can trigger alerts and interventions based on data such as anomalies in patient vital signs.

- **Diagnostics Support**: AI applications in medical imaging and other clinical tests can help doctors identify conditions such as breast cancer, brain injury, or heart disease earlier and more accurately. Such tools can not only improve patient outcomes but also save money. Earlier diagnosis and treatment of many cancers, for example, can cut treatment costs by more than 50%.

- **Treatment Pathways and Support**: Health care professionals can use AI tools to create individualized treatment plans that support VBHC by reducing risk, improving outcomes, and cutting costs.

- **Drug Discovery and Development**: AI can improve biopharma R&D productivity, leveraging past screening results and clinical data to help companies identify and develop promising drugs, while also accelerating trial design and recruitment.

“Artificial Intelligence will drive major advances in realizing the vision of value-based health care. It has the potential to detect connections and correlations between medical treatment and patient outcomes in a way that hasn’t been possible before,” says Ryan Gallagher, BCG project leader and coauthor of the article. “That will not only save lives but also potentially help control rapidly rising health care costs.”
LDRA Technology Pvt. Ltd (a subsidiary of LDRA Ltd. UK) announces the fifth edition of its successful Embedded Safety & Security Summit (ESSS) initiative. This annual event is driven by LDRA with support from its partners and clients, from industrial and professional bodies, and from governmental agencies.

ESSS 2019 promises an engaging whole-day experience on all things embedded. Join the industry’s experts from across the world in Bengaluru on 23 July or Pune on 25 July, to discuss the latest happenings shaping the safety-and-security landscape of embedded technology. Across all sectors, the burgeoning safety-and-security market can be difficult to navigate if you do not apply globally accepted and emerging safety and security standards, methodologies and technologies,” said Ian Hennell, Operations Director at LDRA. “ESSS provides the ideal forum to reflect upon real-world scenarios, share best practices and engage with cutting-edge technology players and thought leaders.”

Themed ‘Enabling a Safe and Secure Tomorrow’, highlights of ESSS 2019 include:

- An Embedded Safety and Security track, targeting the aerospace and defence, and industrial sectors
- An Automotive Functional Safety and Security track
- More that 25+ expert presenters from industry
- Over 900+ delegate technology executives

Initial set of Expert Speakers Announced for Embedded Safety and Security Summit

The first lineup of speakers from the world of Embedded Safety and Security arena is confirmed for the fifth edition of Embedded Safety & Security Summit (ESSS) – 2019. Embedded Safety & Security Summit is a leading technology conference for engineers, senior professionals, decision-makers, regulators, government agencies, thought-leaders, architects and other technologists put together by LDRA India. It has emerged as a must-attend event in the Embedded Safety and Security arena. The theme for this year’s conference is ‘Enabling a Safe and Secure Tomorrow’ with two tracks showcasing on:

(a) Embedded Safety & Security
(b) Automotive Functional Safety & Security

The first set of eminent presenters include:

- Andrew Banks, Chairman – MISRA C and BSI Software Testing Working Group, Technical Specialist, LDRA UK
- David A. Johnson, CFSE, CSP – Senior Safety/Security Engineer, Exida USA
- Anand Deshpande – Senior Deputy Director and Head of Automotive Electronics Department & ARAI’s Centre of Excellence on E-mobility
- Ramesh Babu, H. T, Senior Manager – Functional Safety Engineering, Harman International
- Jay Thomas – Director- Field Engineering, LDRA USA.

Also, experts from companies like Green Hills, ETAS, Tasking, etc. are expected to join this list soon.

Shinto Joseph, Director – South East Asia Operations, LDRA India said, “The summit offers an opportunity for industry players and academicians to meet and discuss current happenings/trends in the industry. This year, with close to 1000 specialized experts coming together, we expect the 5th Edition of ESSS to be one of the largest and focused global conference in our domain.”

ESSS 2019 will exclusively have six technical sessions in each of its track to run parallelly under two themes:

Design & Development
V&V and Certification

These exhaustive sessions cover a wide range of topics relevant to safety-and-security critical software development and are proven to draw together experts from Aerospace, Defence, Industrial, Nuclear and Automotive sectors.

The summit is hosted in the two prominent cities of Bengaluru and Pune. “Fifth edition of Embedded Safety & Security Summit in India has become a pacesetter in embedded domain contributing in achieving a safer and secure tomorrow,” noted Ian Hennell, Operations Director at LDRA UK.

For more details about ESSS 2019 visit at: http://www.embedded-safety-security.com
Blockchain, despite the hype surrounding it, has some way to go before materializing in real-world applications beyond cryptocurrency, primarily due to an amalgamation of numerous factors stemming from the technology’s immaturity, making it inaccessible to those wishing to explore it. The advent of blockchain as a service can change that, allowing blockchain ideas to come into mainstream adoption.

From ensuring food safety and securing patient health records to revolutionizing the gaming industry, the potential ubiquity of blockchain seems imminent. And thus, naturally, businesses from across the world are conceptualizing new blockchain-based applications. They are even engaged in a patent war, and the number of patents for novel blockchain-based applications continues to pile up every day. However, the filing of patents doesn’t necessarily translate to real-world adoption.

While the theoretical applications of the technology abound in the global tech community, successful real-world applications of blockchain seem rare, if at all existent. In fact, business leaders and CIOs are admittedly coming to the realization that the adoption of blockchain has been harder than expected. A Gartner survey revealed that only 1% of CIOs reported any investment in and adoption of blockchain in their organization, while a whopping 77% of businesses have no interest in or no action planned for blockchain adoption at all. Read on to know the reasons for this anticlimactic transition of blockchain from theory to practice, and how creating and offering blockchain as a service can accelerate the mainstream adoption and propagation of the technology.

**Why blockchain adoption is slow**

Although nearly the entire mainstream population, especially tech enthusiasts, business people, and innovators are familiar with the concept of blockchain not everyone knows much about the technology. Even within the tech community, excluding blockchain engineers and researchers, very few people know the nature of blockchain, the capabilities it offers, the limitations that are immanent to the technology, and the applicability of blockchain to different problems. And this lack of knowledge regarding blockchain is the primary cause of the uncertainty and consequently, the sluggish progress in terms of the practical use of the technology.

Currently, there is a short supply of engineers, coders, and researchers that specialize in, or at least have considerable knowledge of blockchain technology. This skill shortage means there are limited opportunities for implementing the applications of blockchain in real-world scenarios. Only organizations who have the requisite knowledge base can proceed with blockchain technology. Add to that the fact that the technology itself is immature and riddled with intrinsic limitations means that highly ambitious projects based on blockchain cannot be implemented.

And businesses that are limited in terms of funds cannot direct their resources towards a technology which is just emerging from its nascent phase and undergoing constant change, which may prove to be risky. And blockchain is a resource-intensive endeavor, which requires not only specialized software knowledge but also is taxing on hardware resources (the very essence of blockchain is a network of multiple computers that need to work simultaneously), which not all organizations possess. This limits the applicability of blockchain projects to only the select few organizations that have the resources to invest in blockchain projects.

So, in short, the accessibility of blockchain is mainly impacted by the steep requirements of the technology itself combined with the lack of resources — both in terms of finance and knowledge. Blockchain technology can be made more accessible if enterprises can offer blockchain as a platform for customers to create and explore their application ideas to expedite the mainstream adoption of the technology.

**What is blockchain as a service**

Blockchain as a service refers to the business model where the owner of a blockchain network offers it as service to customers who can use the blockchain to create and operate their own applications. This allows small short-funded and risk-
averse businesses to experiment with and benefit from applications based on blockchain and smart contracts. The blockchain service providers handle the development and maintenance of the blockchain infrastructure while managing all the back-end operations on the blockchain systems.

Tech industry giants like IBM, Amazon Web Services (AWS), Oracle and a few others have already forayed into the new field of blockchain as a service or BaaS, and are offering smaller players an opportunity to capitalize on the technology. These technology providers, who already provide their technology solutions, mainly packaged as Software-as-a-service (SaaS), are also enabling their blockchain platforms to integrate with their existing software products and information systems. Such features are the mere ability to test a cutting edge technology in its nascent stages is encouraging more and more small and medium enterprise, not to mention a few major non-tech corporations to avail blockchain as a service.

**How blockchain as a service can improve its accessibility**

Offering blockchain as a service to enterprises seeking to test it can easily do so without worrying about the possibility of failure and consequent loss. A major roadblock for businesses wanting to explore blockchain technology was the heavy cost of developing a blockchain system and the risk of losing that investment in case of failure. This roadblock has been eliminated since BaaS providers shoulder both the costs and the risks associated with implementing the fairly immature technology.

These corporations can afford to take the gamble on blockchain and also have the resources to ensure the development of the technology with minimal likelihood of failure. Besides, betting on blockchain isn’t entirely a gamble, as the technology has already proven its potential value in numerous applications, mainly in the finance, insurance, and legal industries. Additionally, these early investors in blockchain stand to gain a major share of the revenues generated by blockchain which is projected to hit $10.6 million dollars by the year 2023.

In addition to having the funds and BaaS providers, who own and attract arguably the brightest talent in technology, consequently, possess enough knowledge and expertise to execute blockchain projects with greater certainty and effectiveness. This minimizes the chances of failure, and the conglomeration of blockchain talent can also potentially expedite the development of blockchain technology ushering the technology into mainstream adoption. Offering blockchain as a service also gives the service providers new revenue streams and the opportunity to enhance their existing SaaS solutions to provide maximum value to customers.

The minimization of the cost of development and the potential risk of failure, combined with the benefits promised by the technology itself makes blockchain an appealing prospect for customers. This not only makes blockchain more accessible but makes its adoption imperative as every business would want to gain a competitive edge over their peers in the form of early adopters’ advantage.

Thus, the existing trend of offering blockchain as a service is set to create a win-win situation for both parties involved — the service providers get the opportunity to generate massive revenue streams while the customers get to experience the benefits of blockchain. Additionally, the technology itself would undergo rapid development as a variety of use cases would come to life, giving future adopters valuable sources of reference for their own projects. This will further lead to accelerated growth in both the complexity, the size, and the number of blockchain projects. It is no surprise then, that the blockchain as a service market is set to hit an incredible $30 billion by as soon as 2024.

**Microsoft announces ‘Week of AI’ to upskill developers and organizations on AI**

A series of virtual workshops on latest trends and key insights into machine learning and AI tools.

5-day program to be addressed by data scientists and tech leaders from Microsoft, Flipkart, Reliance Jio and InMobi.

Microsoft has announced the launch of a specially curated online Artificial Intelligence (AI) program aimed at enabling the developer community and workforces across organizations across India to harness the power of AI. To be held from May 27- May 31 2019, the program will comprise a series of workshops to help participants build their skills and expertise in cloud computing, data sciences, AI and IoT. Additionally, it will also offer insights into the latest trends in AI across the world.

Candidates can to register for the program, which is free of cost, here : Microsoft Week of AI.

The sessions will be addressed by data scientists and AI experts from companies such as Flipkart, Reliance Jio, and InMobi that are leading the way in transforming their businesses and the industry with technology.

Dr. Rohini Srivathsa National Technology Officer – Microsoft India said, “Today, every company is a software company. They have actionable data residing with them but probably lack the expertise or solutions to use it, and with the ever evolving ecosystem it becomes important for these organizations to leverage AI to add business value to end customers and adopt a work culture that has AI deeply integrated. With these virtual sessions, we aim to address the existing gap related to AI skills in Indian businesses. With experts from Microsoft and other industry leaders coming together, we are hopeful of imparting AI and ML skills to a larger talent pool.”
The rollout of better connectivity with 5G and Wi-Fi 6 is a once-in-a-generation gamechanger and I predict an explosion of innovation as a result. We’ve seen it before; when connectivity improves there is an accompanying wave of new products, services and experiences in all of the adjacent industries; and in networking, that’s a lot! The difference between the upcoming wave of innovation and the one we experienced with 4G and LTE is ‘who will be leading the charge’.

4G revolutionized the consumer experience, providing the wireless foundation for the invention of the smartphone putting the internet into our pockets. The introduction of the smartphone then prompted the development of millions of apps that we access multiple times a day to share photos, find a restaurant, pay bills and accomplish virtually any task or access any service from the palm of our hand. Now, we live with our smartphones always within arm’s reach and demand faster and more reliable connectivity as we use the multitude of services on our device. It has been the individual consumer that has forced businesses – and even entire industries – to adapt.

5G and Wi-Fi 6 represent the next major leap in connectivity.

Hate when you’re at a concert or sporting event and can’t immediately post a video to your story or get a message to a friend, or when you move to a far corner of the office and lose internet access? That’s because today’s wireless access points and 4G cells can’t handle the number of devices trying to connect simultaneously. Wi-Fi 6 delivers up to 400% greater capacity and is far more effective in crowded settings. Latency is also reduced allowing faster posting, downloads and loading of apps or webpages. This improved connection will also be less draining on connected device’s batteries making them up to four times more power efficient.

The 4G era brought the digital and physical worlds together through a consumer device – the smartphone. This caused massive disruption, as more than one industry found itself completely transformed because consumers could connect and share information in new ways. Many businesses resisted this change until they were forced to adapt, not because of a business opportunity but purely to survive.

The Wi-Fi 6 evolution will be different. As Wi-Fi 6 will reach maturity much quicker than 5G, it will be the enterprise having the opportunity to drive innovation. And they are hungry to do so, as many businesses have figured out how a digital experience can a be a differentiator. They also have more to work with. Lights, fridges, footballs and grapevines are all becoming connected, meaning we can view the world through an entirely new, digital lens. Whether to make operations safe and more efficient, or to offer consumers a more personalized experience, we’ll see companies embrace this transition – not resist it.

The exciting part of all of this is we still don’t know exactly what use cases and applications are going to emerge. That said, I do believe that Wi-Fi 6 will drive innovation in two main areas:

**Immersive experiences**

**IoT at scale**

Imagine if students could gain entirely new understanding of past events by reliving them through virtual reality. I’m sure experiencing a Martin Luther King or Abraham Lincoln speech as if you’re there makes for a more lasting impression on a student. Or a surgeon being able to take detailed scans of a patient and practicing a procedure in virtual reality before ever making a cut. A warehouse can be outfitted with millions of sensors to allow autonomous electric robots and vehicles to fulfill orders and ship products almost instantaneously. All of this becomes together Wi-Fi 6 and 5G Will Bring a Huge Wave of Innovation
possible with Wi-Fi 6’s increased bandwidth and lower latency.

Wired for Wireless: Wi-Fi 6 and 5G offer enormous opportunities for productivity and innovation, but successfully adopting these technologies at scale will be a challenge. These innovations will increase business mobile traffic up to seven times by 2022 and the number of IoT devices will increase to the billions. This makes security more complicated and critical and puts intense pressure on IT to manage and secure a constantly growing network. The businesses that can successfully address each of these challenges will be the ones that thrive in the new wireless era.

Cisco has been re-architecting the network to meet these challenges and unveiled its intent-based networking portfolio to prepare customers for this wireless-first world. With a software-focused approach, the network unlocks data and insights that will enable IT to support the business in real-time. It automates routine tasks and embeds security into the network itself. These efforts are helping customers and consumers capitalize on the opportunities Wi-Fi 6 and 5G offer, while ensuring security and the best user experience in an increasingly connected world.

Cisco also completed Wi-Fi 6 connection tests with Intel and Samsung to address the inevitable issues that come with a new standard. New Wi-Fi 6 access points across Cisco’s Catalyst and Meraki portfolios offer custom, programmable chipsets and access to industry-leading analytics capabilities for businesses. These new APs deliver a more secure wireless network and can communicate with multiple IoT protocols, including BLE, Zigbee and Thread.

We’re also introducing a new core switch for the campus network. For 20 years, the Catalyst 6000 family of switches has served as the very foundation of many customer campus network. It has been one of the most successful, innovative networking products in the history of the Internet. But businesses today require a networking foundation that is built to solve the challenges posed by our new wireless-first world. The new Catalyst 9600 core switch will do just that and will be the foundation for our customer campus networks for many years into the future.

An explosion of innovation is coming. Is your business ready to lead the charge?
C-suite Beware: You are the latest targets of cybercrime, warns Verizon 2019 Data Breach Investigations Report.

- C-level executives increasingly and proactively targeted by social breaches – correlating to a rise of social-engineering attacks with financial motivation.
- Compromise of web-based email accounts using stolen credentials (98 percent) rising - seen in 60 percent of attacks involving hacking a web application.
- One quarter of all breaches still associated with espionage.
- Ransomware attacks still strong, accounting for 24 percent of the malware incidents analyzed and ranking #2 in most-used malware varieties.
- 12th edition of the DBIR (Data Breach Investigations Report) includes data from 73 contributors, the highest number since launch.
- Analyzes 41,686 security incidents, and 2,013 confirmed breaches from 86 countries.
- C-level executives, who have access to a company’s most sensitive information, are now the major focus for social engineering attacks, alerts the Verizon 2019 Data Breach Investigations Report.

Senior executives are 12x more likely to be the target of social incidents, and 9x more likely to be the target of social breaches than in previous years – and financial motivation remains the key driver. Financially-motivated social engineering attacks (12 percent of all data breaches analyzed) are a key topic in this year’s report, highlighting the critical need to ensure ALL levels of employees are made aware of the potential impact of cybercrime.

“Enterprises are increasingly using edge-based applications to deliver credible insights and experience. Supply chain data, video, and other critical – often personal – data WILL be assembled and analyzed at eye-blink speed, changing how applications utilize secure network capabilities” comments George Fischer, president of Verizon Global Enterprise. “Security must remain front and center when implementing these new applications and architectures.

“Technical IT hygiene and network security are table stakes when it comes to reducing risk. It all begins with understanding your risk posture and the threat landscape, so you can develop and action a solid plan to protect your business against the reality of cybercrime. Knowledge is power, and Verizon’s DBIR offers organizations large and small a comprehensive overview of the cyber threat landscape today so they can quickly develop effective defense strategies.”

A successful pretexting attack on senior executives can reap large dividends as a result of their – often unchallenged – approval authority, and privileged access into critical systems. Typically time-starved and under pressure to deliver, senior executives quickly review and click on emails prior to moving on to the next (or have assistants managing email on their behalf), making suspicious emails more likely to get through. The increasing success of social attacks such as business email compromises (BECS – which represent 370 incidents or 248 confirmed breaches of those analyzed), can be linked to the unhealthy combination of a stressful business environment combined with a lack of focused education on the risks of cybercrime.

This year’s findings also highlight how the growing trend to share and store information within cost-effective cloud based solutions is exposing companies to additional security risks. Analysis found that there was a substantial shift towards compromise of cloud-based email accounts via the use of stolen credentials. In addition, publishing errors in the cloud are increasing year-over-year. Misconfiguration (“Miscellaneous Errors”) led to a number of massive, cloud-based file storage breaches, exposing at least 60 million
Ransomware attacks are still going strong:

They account for nearly 24 percent of incidents where malware was used. Ransomware has become so commonplace that it is less frequently mentioned in the specialized media unless there is a high profile target.

Media-hyped crypto-mining attacks were hardly existent:

These types of attacks were not listed in the top 10 malware varieties, and only accounted for roughly 2 percent of incidents.

Outsider threats remain dominant:

External threat actors are still the primary force behind attacks (69 percent of breaches) with insiders accounting for 34 percent.

Putting business sectors under the microscope:

Once again, this year’s report highlights the biggest threats faced by individual industries, and also offers guidance on what companies can do to mitigate against these risks.

“Every year we analyze data and alert companies as to the latest cybercriminal trends in order for them to refocus their security strategies and proactively protect their businesses from cyber threats. However, even though we see specific targets and attack locations change, ultimately the tactics used by the criminals remain the same. There is an urgent need for businesses – large and small – to put the security of their business and protection of customer data first. Often even basic security practices and common sense deter cybercrime,” comments Sartin.

Industry findings of note include:

Educational Services: There was a noticeable shift towards financially motivated crime (80 percent). 35 percent of all breaches were due to human error and approximately a quarter of breaches arose from web application attacks, most of which were attributable to the use of stolen credentials used to access cloud-based email.

Healthcare: This business sector continues to be the only industry to show a greater number of insider compared to external attacks (60 versus 42 percent respectively). Unsurprisingly, medical data is 18x more likely to be compromised in this industry, and when an internal actor is involved, is it 14x more likely to be a medical professional such as a doctor or nurse.

Manufacturing: For the second year in a row, financially motivated attacks outnumber cyber-espionage as the main reason for breaches in manufacturing, and this year by a more significant percentage (68 percent).

Public Sector: Cyber-espionage rose this year – however, nearly 47 percent of breaches were only discovered years after the initial attack.

Retail: Since 2015, Point of Sale (PoS) breaches have decreased by a factor of 10, while Web Application breaches are now 13x more likely.

More data from highest number of contributors ever means deeper insights:

“We are privileged to include data from more contributors this year than ever before, and had the pleasure of welcoming the FBI into our fold for the very first time,” adds Sartin. “We are able to provide the valuable insights from our DBIR research as a result of the participation of our renowned contributors. We would like to thank them all for their continued support and welcome other organizations from around the world to join us in our forthcoming editions.”

This is the 12th edition of the DBIR and boosts the highest number of global contributors so far – 73 contributors since its launch in 2008. It contains analysis of 41,686 security incidents, which includes 2,013 confirmed breaches. With this increase of contributors Verizon saw a substantial increase of data to be analyzed, totaling approximately 1.5 billion data points of non-incident data.

This year’s report also debuts new metrics and reasoning which helps identify which services are seen as the most lucrative for attackers to both scan for and attack at scale. This analysis is based on honeypot and internet scan data.
NetApp and Zinnov today announced the results of their first-of-its-kind study titled, ‘B2B Tech Startup Ecosystem and Role of Corporate Accelerators in India’. Have grown by 3X from 800 to over 3200
Have seen a surge in funding, up by 364% to US$3.7Bn in 2018
Are mostly present in the top 3 startup hubs: Bangalore, Mumbai and Delhi NCR
Take advantage of the 50+ corporate accelerator/incubator programs to build maturity
NETAPP-ZINNOV Study Findings reveal that B2B tech startups in the last 5 years (2014-18)
The complete report can be downloaded here: https://startup.netapp.in/news-blogs-events/

NetApp, a leader in data management and hybrid cloud, in partnership with Zinnov, a global management consulting firm, today announced the results of their first-of-its-kind study titled, ‘B2B Tech Startup Ecosystem and Role of Corporate Accelerators in India’. The study provides data-driven insights into the growth of B2B tech startups and the upsurge in both funding as well as the corporate accelerator programs in India over the last five years. “The report is jointly developed by NetApp and Zinnov Management Consulting through a detailed study to understand the B2B tech startup landscape and the rise of corporate accelerator programs in India. During the study, the research team conducted both primary and secondary research for analysis and key insights”.

According to the report, B2B tech startups have more than tripled (from 900 to 3200+) since 2014. This can largely be attributed to the spurt in the need for digital transformation of enterprises, financial institutions, hospitals, government, SMEs, etc. Adding fuel to their success is the growing investor interest – the investment in B2B startups touched US$3.7 billion in 2018, a steep rise of 364% from 2014.

Commenting on this trend, Sanjay Nath, Co-Founder and Managing Partner at Blume Ventures, said, “The B2B startup wave in India has just begun. Corporates are more open to collaboration with startups, VC firms are more interested in the B2B startup world, and technologies like AI and IoT have proliferated faster into the B2B ecosystem, compared to B2C. This holy combination of corporate support, B2B focused VC funds, and rise of advanced technologies will drive the wave forward.”

The report further unveils that 70% of these B2B tech startups are in the space of enterprise tech (41%), fintech (19%) and healthtech (9%), with software as a service (SaaS), customer relationship management (CRM), alternative lending, expense management, medical internet of things, artificial intelligence enabled predictive platforms being some of the other segments.

Advanced B2B tech startups dabble with 3D printing, blockchain and robotic process automation
Segregating over 800 of the B2B tech startups as ‘advanced tech startups’, the study indicates their YoY growth at 60%, much ahead of the 20% number for the entire tech startup space (B2B, B2C). More than 76% of the tech share belongs to the top trio: Data Analytics, Artificial Intelligence and Internet of Things. Other futuristic technologies such as blockchain and 3D printing are not just being adopted by enterprise tech, but also fintech, healthtech, industrial-tech, clean-tech, manufacturing and nanotechnology.

Corporate incubators and accelerators are emerging as the backbone of startup tech
Currently, there are over 50 corporate accelerators and incubators in the country, focusing on technologies such as AI/ML, Big Data, Cloud, Blockchain, Cyber Security among others. These include the likes of NetApp, Cisco, Target, Intel and Swiss Re. While global accelerators hold a majority with 66% of the share, 34% of the pie comprises of Indian companies. Varied in their philosophy, the accelerators have an aim to offer support in the form of market access, mentorship, investor connects and access to product platforms.
Alluding to the vital support that corporate accelerators provide, Ajeya Motaganahalli – Senior Director and Leader, NetApp Excellerator, NetApp, said, “It is encouraging to see the entrepreneurship explosion across the startup universe. At NetApp Excellerator, we’ve facilitated numerous go-to-market opportunities, helped startups secure several million dollars in funding and have formed 7 global strategic alliances in the two years of our operation. This shows the credibility that the accelerator programs can add to such startups.”

Favourable conditions that make India a hotbed for B2B tech startups

Bangalore is the top city for B2B tech startups followed by Delhi NCR and Mumbai, all accounting for about 60% of all B2B tech startups. Presence of huge number of MNCs, access to technology, extensive talent pool, plus a strong presence of incubators and accelerators are key to the consistent startup growth in Bangalore (800+), whereas top institutes like IIT Delhi and Delhi University have fostered startups in various verticals across Delhi and NCR (550+). Mumbai (400+) being the financial hub, is home to the largest fintech startups.

Pari Natarajan, Co-Founder and CEO, Zinnov, said, “There has never been a better time to be a technology entrepreneur in India than now. The incredible rise in the number of B2B startups as a percentage of the total tech startups from 26% in 2014 to 43% in 2018, is a testament to this. Our study found that funding chances increase by 3X after startups graduate from an incubator/accelerator. An intense growth of accelerators and incubators is the much-needed shot in the arm for Indian startups to spread their wings across the length and breadth of the country, encouraging tier 2 and 3 cities to come up.”

“Businesses require new age data-driven technologies in order to stay ahead in the competition curve. We will continue to provide innovation centric mentoring to help new age startups maximize their potential for business globally,” concluded Ajeya Motaganahalli.

With flexible economic policies, state government support and access to various industries, Hyderabad, Pune and Chennai accounting for 500+ startups collectively are posited as the growing startup hubs of the country.

Android Pie: Everything you need to know about Android 9

Android P is officially Android 9 Pie. No Popsicles or Pineapples here. On August 6, 2018, Google revealed that its next version of Android is Android 9 Pie.

Along with the name change, the number is also slightly different. Rather than following the trend of 7.0, 8.0, etc., Pie is referred to as 9. This probably doesn’t mean much in the grand scheme of things, but it’s still an interesting move on Google’s part.

Android Pie isn’t as drastic of a visual change like we saw with the jump from KitKat to Lolipop, but compared to Oreo, there are some elements that are noticeably different.

At first glance, things like the colorful icons in Settings, circular Quick Settings icons, and rounded corners for just about every menu jump out like a sore thumb. These elements do take some getting used to, but I ultimately came around to liking them quite a bit.

Something else you’ll notice with Pie is just how alive it feels. Between the new gestures and updated animations, Android moves in a way that I’ve never seen before. Oreo was smooth and buttery, but Pie flies underneath your fingertips in a way that can only be experienced in-person.

You’ll also find a feature called App Timers that’ll restrict you from using a certain app after you’ve spent x amount of time on it, as well as tools for easily turning on Do Not Disturb and switching your screen to a monochrome color palette to help you wind down for bed.

It seems like Google’s always trying to find ways to maximize your phone’s battery life as much as possible, and with Android Pie, those efforts are present in a new Adaptive Battery mode.
By Preston Gralla, Technical Writer, Symantec

As enterprises look to secure their infrastructures against attacks, many continue to fall prey to basic errors. Here’s how to sidestep potential pitfalls.

Enterprises spend countless amounts of time and money on sophisticated cyber security techniques. But sometimes the biggest security mistakes they make are hiding in plain sight. If you’re looking to keep your company as safe as possible from cyber attacks, here are five common security mistakes to avoid.

Mistake No. 1: Playing Fast and Loose with Admin Accounts

Your enterprise likely has plenty of admin accounts, giving some employees unfettered control over vital hardware and services. And that spells danger, says Rob Clyde, managing partner at Clyde Consulting and the chair of the board of directors for the non-profit ISACA information security organization.

Clyde calls admin accounts “the soft underbelly of every organization.” He explains, “Admins have full privileges and often have access to the keys to the kingdom in the virtual and cloud environments. That means a hacker who gains access to an admin account can literally take down an entire enterprise. And yet attacks targeted at admins are commonly overlooked.”

He recommends that organizations dial back on their number of admin accounts and make sure only those who need them, get them. He also suggests adding granular security, so that each account only gets access to the resources they truly need to do their work.

Finally, according to Clyde, enterprise should consider requiring secondary approval for some tasks, such as deleting all virtual machines or containers. That way, even if hackers gain access to an admin account, they won’t be able to do as much damage, because other admins in the organization have to sign off on high-risk actions.

Mistake No. 2: Forgoing a Comprehensive Risk Management Framework

Companies often build a set of security systems and procedures, but don’t take into account how cyber risks affect the entire organization. So cyber security is seen as purely a technical issue that requires attention from only the IT department, rather than the entire enterprise. The result?

Enterprises are less secure because not every group and individual may be aware of cyber dangers and be on guard against them. So says Chris Dimitriadis, the past chairman of the ISACA Board of Directors.

Dimitriadis says a comprehensive risk management framework needs to clearly outline how cyber risks translate into business risks, and how they can affect the company. The stakes are high as organizations may risk millions of dollars in reputational costs and lost customer trust. That way, the entire company, from the board of directors on down, will be aware of risks and be more likely to avoid them.

Mistake No. 3: Not Patching

You’ve probably heard this one more times than you heard as a kid being reminded to eat your spinach – No matter: Make sure to keep your systems patched and up to date. Clyde and Dimitriadis both underscore the importance of what ought to be a routine part of a company’s preventive security routine. Yet too many organizations still forget to incorporate this as standard practice. There are countless examples of unpatched vulnerabilities leading to successful cyber attacks, with damages literally adding up to hundreds of millions of dollars.

“The bad guys know what all the vulnerabilities are —it’s public information,” Clyde says. “The exploits are out there for all to see and use on the Internet. So you’ve got to be vigilant in keeping systems up to date.”

Mistake No. 4: Ignoring IoT Device Security

It’s easy for companies to forget that their IoT devices, such as sensors and surveillance cameras, are a very large and very tempting target for hackers and can be easily exploited. Clyde says companies need to treat them with the same kinds of security as they do servers and other IT-related systems. That means not just
making sure they’re protected by things like firewalls, but also keeping them patched and changing their default passwords. Even that might not be enough, he says. IoT manufacturers are notorious for ignoring security, and some devices are inherently insecure — they might have default passwords that can’t be changed, or the devices can’t be automatically updated. So companies should check every IoT device they own, and if they can’t be kept secure, “Throw the device away and replace it,” Clyde says. In addition, companies should make sure any new IoT device they buy can be adequately protected.

Mistake No. 5: Skimping on Training

The best protection against hackers and data breaches is a workforce educated in cyber security dangers. But while this is the organization’s first line of defense, the vast majority of companies haven’t instilled a solid cyber security culture. Clyde points to a 2018 study by ISACA in which 95 percent of security professionals surveyed said there’s a gap between the security culture their company wants — and the security culture they have.

The best way to instill a culture of cyber security awareness is through training. And training doesn’t mean one-and-done seminars that employees reluctantly attend, and then immediately forget about. It means active, ongoing work.

“Anti-phishing training is particularly important because of how frequently it’s the way companies are breached,” according to Clyde. “For training to be successful, you’ll need to send non-harmful, phishing emails to employees and then measure how they responded. How many actually fell for the bait and clicked? And then do more training, until people respond properly.”

The number of smartphone users in the country is expected to double to 859 million by 2022 from 468 million users in 2017 growing at a compound annual growth rate (CAGR) of 12.9%, according to an ASSOCHAM-PwC joint study. As of 2017, the number of smartphones in the country stood at 468 million and likely reach 859 million smartphones users by 2022. The non-smartphone ownership in India will decrease from 701 million in 2017 to 504 million in 2022 at a CAGR of -6.4% as more and more people opt for smartphones, noted ASSOCHAM-PwC joint study on ‘Video on Demand: Entertainment reimagined’.

With lower than ever data tariffs and increasing smartphone penetration in the country, it is safe to assume that the VoD market will be a significant beneficiary of these developments. Internet consumption is clearly on the rise in India. The important factor for the VoD industry is the availability of devices that are compatible with online video viewing. A large volume of consumption occurs on smartphones, noted the joint study. Tablets are another promising device for the VoD industry. However, India has just about 5.3% penetration as of 2017, and this is expected to go up to just about 10% in 2022. The low penetration is definitely a missed opportunity for players as tablets offer fairly larger screens which are better for consuming HD content as compared to smartphones.

Television is the largest sub-segment within the entertainment and media industry and will continue to remain so in the near future. While the Indian television industry is set to grow from 13,314 million USD (8,66,181 million INR) in 2017 to 22,003 million USD (14,33,137 million INR) in 2022 at a CAGR of 10.6%, the global growth average is as low as 1.4%. This proves that India will continue to ride on traditional forms of entertainment despite the disruption in the industry. Television is one of the most economical forms of content consumption, making it a popular source of entertainment for rural India, noted the joint study.

With a CAGR of 22.6% during the period of 2017–2022, the Indian video OTT market is poised to outperform the global video OTT market, which is pegged to have a CAGR of 10.1% during the same period. Also, by 2022, the Indian video OTT market will be amongst the top 10 markets globally with a market size of 823 million USD (53,630 million INR), highlighted the joint study.

Low data tariffs and increasing smartphone penetration have ensured that consumers and their devices are always connected and on. Mobile devices are becoming the consumer’s preferred choice to consume content. This has made it crucial for content creators and distributors to tailor their content and services for the mobile consumer.
Kaspersky Lab experts detected a blast of sophisticated spam emails in the first quarter of 2019, featuring fake job-offers that seemed to come from HR-recruiters in large corporations that traditionally attract a lot of interest from potential employees. However, the emails actually came from spammers and installed money-stealing malware on users’ devices.

Spam emails are an often underestimated threat, yet they can spread malware through social engineering methods like deception and psychological manipulation, and claim many victims. To track such emails, Kaspersky Lab researchers use honeypots – virtual ‘traps’ able to detect malicious emails and catch threat actors. For this particular operation, they tracked fraudsters trying to exploit unwary people looking for a new role.

Analysis of the findings from the honeypots is included in the new Spam and Phishing in Q1 2019 report. This shows that recipients of the spam emails were offered a tempting position in a large company. They were invited to join a job search system for free by installing a special application on their device that would provide access to the job-search database. To make the installation process look trustworthy, the attackers accompanied it with a pop-up window carrying the words “DDoS Protection” and a fake message that claimed the user was being redirected to the website of one of the largest recruitment agencies. In fact, victims were redirected to a cloud storage site from where they would download a malicious installer that looked like a word file. Its function was to download to the victim’s machine the infamous Gozi banking trojan, one of the most commonly used malware for stealing money. Kaspersky Lab detects it as Trojan-Banker.Win32.Gozi.bqr.

“We often see spammers using names of large and well known companies – it helps them to succeed in their malicious business and gain people’s trust. Famous brands with a solid reputation can become victims of fraudsters who pretend to be them and lure unsuspecting users into downloading a malicious attachment to their computers. This particular scheme involved the names of both well known recruiting companies and respected businesses, which made it even more sophisticated. One needed to check the email address line for errors to suspect that the job offer was not authentic,” said Maria Vergelis, a security researcher at Kaspersky Lab.

To avoid falling victim to malicious spam, users are advised to:

- Always check the web address of a website you are redirected to, or the link address and the sender’s email, to ensure they are genuine before clicking on them, and make sure that the name of link in the message doesn’t cover another hyperlink.
- Do not click on links in emails, texts, instant messaging or social media posts if they come from people or organizations you don’t know, or have suspicious or unusual addresses. Make sure they are legitimate and start with ‘https’ whenever any personal or financial information is asked for.
- If you are not sure that the company website is real and safe, never enter your personal information.
- Check the company’s official website for open vacancies matching your job skills.
- Make an additional phone call to the company to be sure that the job-offer is real.
- Review your job-offer for possible mistakes: carefully check the company name or job title and responsibilities.
- Use a reliable security solution for comprehensive protection from a wide range of threats, such as Kaspersky Security Cloud

Other findings of the report include:

**Phishing**:

In Q1 2019, the Kaspersky Lab’s anti-phishing module prevented 111,832,308 attempts to direct users to scam websites. This is a 24% increase compared to the Q1 2018 figure, which was 90,245,060.

The banking sector has become the number one target, followed by global internet portals and payment systems.

Brazil was the country with the largest share of users attacked by phishers in the first quarter of 2019 (22% compared to 19% in Q1 2018). It was followed by Austria (17%) and Spain (17%).

**Spam**:

In the first quarter of 2019, the amount of spam peaked in March (56.3%). The average share of spam in the world’s email traffic was 56%, which is 4% more than in Q1 2018.

China (16%) was the most popular source of spam, followed by the United States (13%) and Russia (7%).
Please Join us...

5th June, 2019 WORLD ENVIRONMENT DAY

from 6-00am onwards
at PEOPLE’S PLAZA,
Necklace Road,
Hyderabad.

TOWARDS A POLLUTION-FREE PLANET

Organised by:
GREEN-LACE
SOCIETY®
a voluntary organisation

Mob: 8686445666, 9703252044
Email: greenlacesociety@gmail.com, Web: www.greenlace.org
16th International Photography, Videography, Digital Imaging, Frame & Album Exhibition

Photo Today

FRI 28 SAT 29 SUN 30 JUNE 2019
BENGALURU

Forthcoming Shows

19, 20 & 21 July 2019
Chennai Trade Centre
CHENNAI

15, 16 & 17 Nov 2019
BMICH
SRILANKA

For Details Contact: BUYSELL INTERACTIONS PRIVATE LIMITED
Mob: 98840 80051, 90420 32366 / 67, Email: info@buysellint.biz, Web: www.buysellint.com