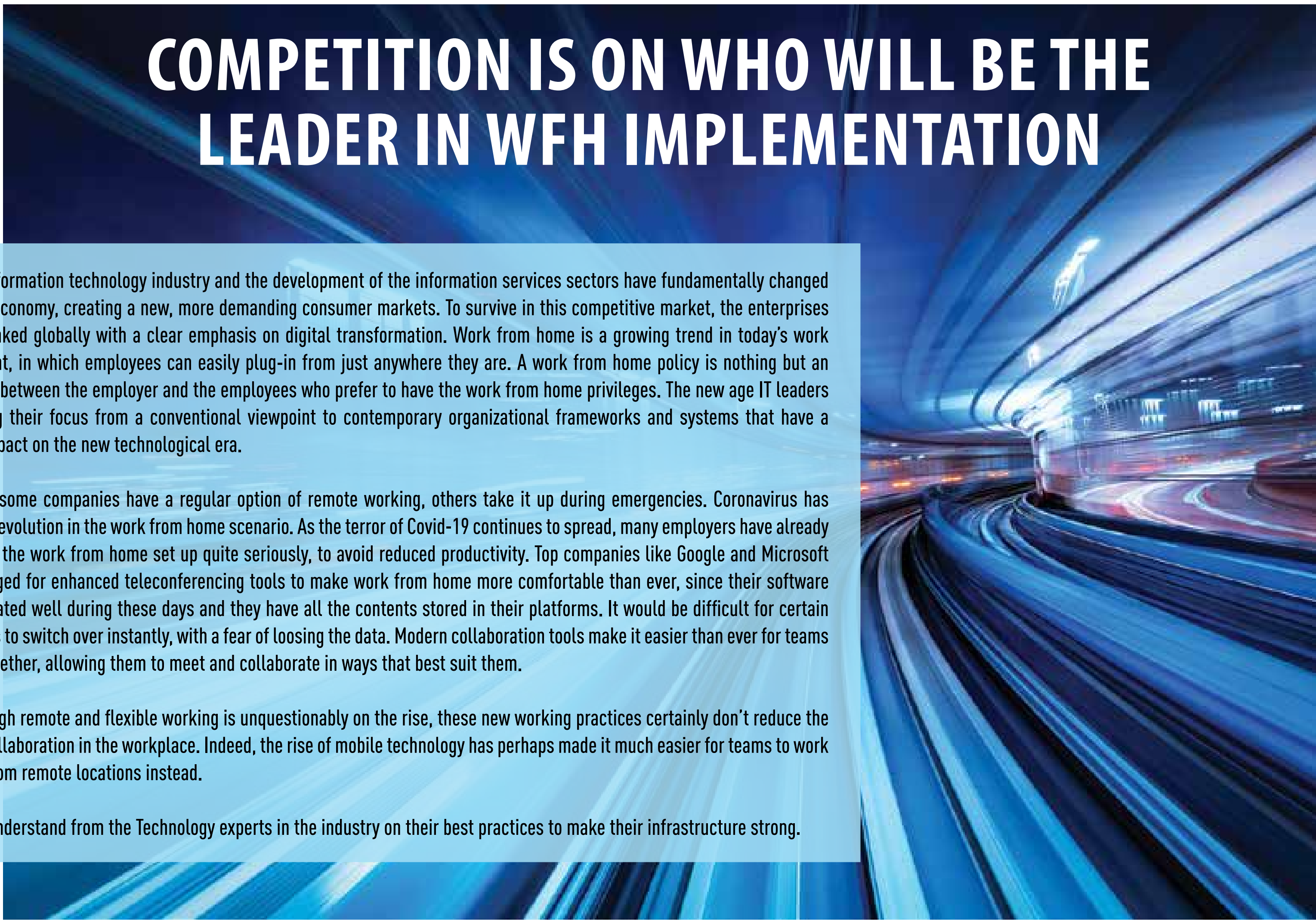
COMPETITION IS ON WHO WILL BE THE LEADER IN WFH IMPLEMENTATION



The information technology industry and the development of the information services sectors have fundamentally changed the world economy, creating a new, more demanding consumer markets. To survive in this competitive market, the enterprises must be linked globally with a clear emphasis on digital transformation. Work from home is a growing trend in today's work environment, in which employees can easily plug-in from just anywhere they are. A work from home policy is nothing but an agreement between the employer and the employees who prefer to have the work from home privileges. The new age IT leaders are shifting their focus from a conventional viewpoint to contemporary organizational frameworks and systems that have a positive impact on the new technological era.

While some companies have a regular option of remote working, others take it up during emergencies. Coronavirus has sparked a revolution in the work from home scenario. As the terror of Covid-19 continues to spread, many employers have already considered the work from home set up quite seriously, to avoid reduced productivity. Top companies like Google and Microsoft have arranged for enhanced teleconferencing tools to make work from home more comfortable than ever, since their software has penetrated well during these days and they have all the contents stored in their platforms. It would be difficult for certain Institutions to switch over instantly, with a fear of loosing the data. Modern collaboration tools make it easier than ever for teams to work together, allowing them to meet and collaborate in ways that best suit them.

Although remote and flexible working is unquestionably on the rise, these new working practices certainly don't reduce the need for collaboration in the workplace. Indeed, the rise of mobile technology has perhaps made it much easier for teams to work together from remote locations instead.

Lets understand from the Technology experts in the industry on their best practices to make their infrastructure strong.

BSE: A FRONTRUNNER IN TECHNOLOGY ADOPTION

KEY PRIORITIES OF 2020

BSE has already implemented some of the most talked about newer technologies, such as Artificial Intelligence, Machine Learning, Automation etc. Our focus for the year 2020-21, is to extend these technologies into more service oriented domains that will help in meeting the compliance requirements, enhancing the end user experience, improve the business processes and turnaround time for our customers through automation.

We also plan to make our services more flexible by on boarding these services in form of mobile applications, mainly in the area of compliance, customer engagement, and enhanced trading interfaces. Together, we have also started introducing micro services in our important business applications. As regards the security, we are pro-actively and continuously upgrading our cyber security infrastructure to meet the never ending challenges of cyber threats. To name one such major activity that we recently performed during the ongoing lockdown period was replacement of our core enterprise firewall, with all teams working remotely from home.

CYBER SECURITY

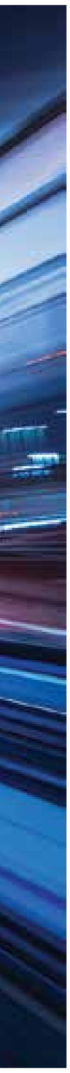
BSE has been identified as the most critical infrastructure by the National Critical Information Infrastructure Protection Centre. Today, BSE is the custodian of information of more than 5500 listed companies and an equally enormous amount of trading and related data it is holding since inception. At no point of time this can be compromised. For this, three years back, BSE procured a total of 27 niche information security technologies, including all advanced technologies like deception technology, NTAPT, forensics, user behaviour analysis, predictive analysis, cognitive tools, Machine Learning tools, SIEM, etc.

ACHIEVING DIGITALIZATION

On the technology front, BSE has implemented many innovative solutions as a leader in the industry and companies are inspired to follow our model. BSE's StarMf platform is just one such example, which has revolutionised the mutual fund distribution business in India. We have shared our implementation in the BigData domain and how effectively the use of different technologies has been extended in our business and compliance requirements. We are also creating our own solutions developed by our in-house IT team, which will be offered as a service. Another example of our engagement in this area is offering Cyber Security expertise to our Trading members as a service viz. Member SOC. In this model, BSE will invest in the infrastructure and technology and this will be available as a service on subscription basis to trading members to analyse their security posture and guide them.

KERSI TAVADIA
CIO
BSE

> "We at BSE, have almost digitalised all our processes by providing a web-based interface for our customers such as submitting documents in form of eKYC, engaged with third parties for digital payments, submission of compliance documents, companies can submit their announcements, financial results, etc. online and same is immediately disseminated on our website."



WHY THE BFSI SEGMENT NEEDS TO BEEF UP ITS CYBER SECURITY INFRASTRUCTURE

SANDEEP KAMBLE
Founder and CTO
SecureLayer7

The Indian BFSI segment has been one of the fastest growing segments in the country, fuelled by fast paced technology adoptions and supportive government policies. The Industrial 4.0 revolution, that integrates smart technology tools with day to day business operations, leveraging AI, ML, and cloud computing etc., making essential functions accessible at the touch of a smart screen, have evolved rapidly. These innovations, integrated with a massive rise in fintech, are helping create a cashless economy for India. As per a report by RedSeer Consulting, India's Digital Payments Market was valued at INR 2,162 trillion in 2019-20 and is expected to grow three fold, to reach INR 7,092 Trillion by 2025. Further, the current 160 million unique mobile payment users are set to multiply 5 times, to reach 800 million, by 2025.

However, with the increased digitisation, the rise in cases of cyber security breaches, have exposed several vulnerabilities. The security breach at the State Bank of India in 2019, for example, exposed the bank account numbers and bank balance information for its 422 million customers. Similar attacks of varying scales have also taken place across various public and private banks in the country, in the past few years. Globally, the BFSI Sector has been witnessing a rise in cyber-attacks where skilled hackers are able to carry out well planned breaches, heists, invasions, data thefts, malware and phishing attacks, etc., resulting in major financial loss and distress. As per a report by the Reserve Bank of India (RBI), around 60,000 cyber frauds took place in the banking sector alone, including the Scheduled Commercial Banks (SCB), during the fiscal year of 2018-19, and resulted in a loss of INR 67, 432 Cr. for the last fiscal. According to a report by CISO, in 2018, the Indian BFSI segment clocked an average B+ OSINT Security score, and was ranked 50 in Security maturity and 42 in breach readiness. Some vital platforms which are most vulnerable and need a cyber-security assessment and action, include:

Solutions by Fintech Start-ups: Over the past few years, a number of technology start-ups specialising in financial segment have emerged, disrupting the way we make purchases. From app based wallets and Aadhaar/ UPI linked instant transactions to single window e-commerce apps, fintech start-ups need to be mindful of the threats and invest in creating a robust data security framework for the apps. This is generally ignored as these may be bootstrapped start-ups and generally avoid hefty investment needed for a more than basic digitally secure ecosystem. This needs to be addressed by collaboration with cyber security firms that provide customised and value driven services, as against the big budget packages.

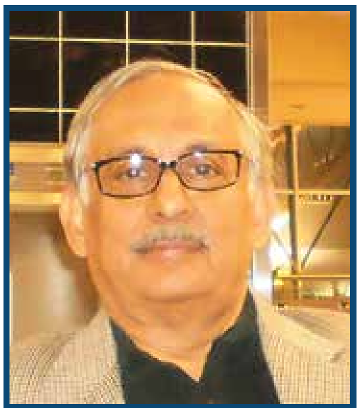
ATM Security: These have been very common and involve a combination of physical breach – where fingerprints and card details are stolen by imprinting the contact point of the machine, and software breaches. As per a report by Positive Technologies, up to 69% of all ATM's are vulnerable to cyber-attacks. Interestingly, ATM attacks have been getting complex and more sophisticated since the first ATM Malware attack of 2018, and it is expected to continue being a looming threat. ATM security assessment, an important exercise, is a recommended mode of addressing these vulnerabilities.

Mobile Apps and Integration: As per a report by Avaya India, 26% of Indian customers regularly avail digital banking services through the bank website and mobile app. With the increased use age of smartphones and the consumer friendly mobile app version for one tap transactions, mobile and digital banking is set to further enhance the vulnerability of the platform. Banks need to pay special attention to these platforms when it comes to cybersecurity.

Social Engineering: Data has become the new currency now and financial data is even more valuable. While innovative and complicated cybercrimes are on a rise, especially for newer platforms, the age old methods of phishing, network scanning, viral code, website defacements and intrusion and the conventional malware also continue to grow, mostly unchecked. These require a consistent effort to monitor using advanced detection technology processes to ensure there are no major or minor compromises.

While all of the above are important steps to be taken by BFSI players, including banks, service providers, fintech players and their technical support staff, a significant aspect of secure transactions is also consumer awareness. With automated messaging alerting consumers to not share their OTP or CVV numbers over a call or to use secure servers when making financial transactions, most banks, and financial institutes are taking basic steps towards educating their customers. However, a strategic, technology expert led awareness campaign can play a significant role in educating masses about effective and secure use of digital platforms for financial transactions, which is the need of the hour as an increasing number of people are now operating from home, through barely secure servers.

"AT THIS TIME, LIKE LOCKDOWN SECURITY OF DATA AT ANY COST IS A MUST"



ALOKE CHAKRAVARTTY
Vice Chancellor
Techno Global University

KEY PRIORITIES OF 2020

We will plan after the pandemic, how to restart the plant and complete mergers.

COMBINING BREAKTHROUGH & FUSION APPROACH

It is an ongoing concern. At present the problem is getting back customers.

CYBER SECURITY

How can you ensure security when everything is so open? Security will become a big issue due to rogue nations. We are thinking of going back to manual for outward communication. There will be delays but that has to be built in the system. At this time, like lockdown security of data at any cost is a must.

> "2020 will be known for survival. Many customers will close down."

CYBER CRISIS MANAGEMENT PLAN: A NECESSITY

ANIL RANJAN
Sr. Practice Lead & Sr. Solution Architect, Inspirisys Solutions

Cyber security incident is a crisis scenario that every organization is vulnerable to. It is almost impossible to protect the business 100% from cyberattacks, but we can create an effective incident response plan that instructs our IT team on how to respond to an attack. Effective crisis management is not the same as cyber incident response. A computer incident could refer to such as malware infection, Application/network disruption involved limited information disclosure and can be handled by incident response plan. Just an information may be provided to CIO/CISO for such incident. Cyber crisis refers to more serious incident that has potential to cause significant financial loss or brand reputation damage and company's top management CEO, COO, CFO, CIO, CISO must be involved.

IT (Information Technology) systems are vulnerable to a different type of threats from a variety of sources such as natural disasters, human error, and hacker attacks. The disruptions due to these threats can be from short-time power outage, hard disk drive failure to severe like equipment destruction, fire, online database hacked. Crisis management planning include those steps to recover IT services from an emergency or system disruption.

Crisis Management Plan and BCP/DR are interrelated but distinct. DR details of procedures and steps to recover from a disaster.

Business Continuity Plan= Crisis Management Plan + DR Plan
Cyber Crisis lifecycle: Pre-Crisis, Crisis phase and Post Crisis.

Pre-Crisis Phase:

Crisis Detection: Detection information may come from external sources, such as – customer complaint, regulator complaint, and any other third party; and also from internal sources like helpdesk team and the team engaged for "Security Incident Management Procedure".

Pre-Crisis Phase includes--- 24*7 monitoring, identifying and creating a crisis team – a group of people working across the business who will be responsible for the strategy and for seeing it through. Appointing expert media trained spokesperson to be interviewed. Identifying employees, shareholders, stakeholders, the public, partners and the media.

Communication templates for breach notifications should be ready, for example for GDPR.

Templates of statements for customers, business partners, media and external agencies should be prepared;

For Banking sector, RBI Guidelines should be followed.

Crisis phase: Management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the organization's response is equal to the situation, through the right channels and via the crisis team – before rumor, incorrect information or negative reactions start to propagate. Being silent is not a good step and people/stakeholder may think as something wrong/hidden thing and organization brand reputation can be damaged.

Need to know whether there was any failure on the part of the organization, either due to a lack of control in its systems, processes, policies or technology. As per situation demand, apology/accepting some responsibility is not a wrong step. Recovery strategy with brief details can be explained. Govt or Law & order maintaining department should be informed as per the severity of crisis and as per company's guidelines.

Need to determine the affected stakeholders and if any data is exposed than need to determine, what data has been exposed, and impact of this. If personally identifiable information (PII) was involved, steps have to follow as per data privacy legal rule. Communication templates for breach notifications should be used as required by applicable privacy laws, for example GDPR

Post-Crisis:

During this phase, companies will take the opportunity to look back and reflect. They do the deep analysis and investigation, RCA (Root cause Analysis) to know the root cause, which helps them to change their policy/procedure, Preventive action for the next crisis. It's a lesson learning also for the company. Lesson learnt database must be created.

Post-crisis, organization should be in touch with the media and different stakeholders to rebuild the relationship and trust. If you've handled the crisis well, there should be latent trust and credibility that you can build on.

CHALLENGES FOR CYBER CRISIS MANAGEMENT PLAN:

1. Company's top management lacks understanding of their role & responsibility in case of Cyber Crisis.
2. Communication plan, trained media Spokesperson is not defined.
3. No guidelines when to communicate to Law & Order govt department,
4. Cyber Crisis Management plan never exercised/tested.
5. Templates of statements for customers, business partners, media and external agencies not prepared.
6. Either there is no insurance coverage for cyber crisis or it's T&C not clearly defined.

MOST VULNERABLE INDUSTRY FOR CYBER ATTACK IN INDIA:

- Banking & Financial
- Power industry
- Manufacturing Industry
- Healthcare

PINE LABS MAKING DIGITAL PAYMENTS EASIER AND SAFER

SANJEEV KUMAR
CTO
Pine Labs

SECURITY & POS TERMINALS

Traditionally the POS terminals have been there, but our POS terminals are very special in the sense that they are highly secure and undergo a lot of security. There are a lot of security standards which they have to follow like PCI compliance and PCA PTS etc.

The POS terminals are literally not open. So what we tried to do was that we created a wrapper on top of the secure OS so that the changes on those terminals will become easier. So if there are a lot of security aspects, then changes are also required to be done and at a lesser frequency because they have to undergo multiple rounds of testing and that is beyond the functional testing, security testing is also required. So we have developed this wrapper platform, what it does is that be it any other terminal you create a wrapper on top of it and you can push the application. For the proprietary payment terminals we have our own application store. Typically you download some applications from Android Play Store and Apple App Store. Similarly, on these terminals we try to write an application store from where you can put the payment application from our central application store for these terminals.

Now there is a culture of open API. So all the payment API's are exposed and you can build any interesting third party app, with Android based POS applications coming up at one side maintaining security, creating our own ecosystem of payment apps, open the platform for everybody to be able to create the app and at the time of payment they just invoke a simple API call to us and they can write a lot of use cases.

Our application store has more than 50 apps cutting across segments, merchant category codes and we have a developer community.

ENCOURAGING DIGITAL INDIA INITIATIVE

Digital India is like, if you talk about movement from cash to card, cash to UPI or wallets. The cash transaction is moving to either online or terminals. We are launching our contactless card acceptance on our Soft POS wherein you can have any Android device which is NFC (Near Field Communication) enabled, our application can be downloaded from the Play Store with the KYC done which is also digitized. So first is digital KYC, then on boarding the merchant instantly, then merchants can start transacting instantly. So whatever was happening on cash or the merchants who did not have the card acceptance machine suddenly all of them can join this. So any phone having NFC can download the ePOS app, it is going to be launched soon. Suddenly our coverage increased and these things definitely add to the Digital India initiative. Now there are transactions like offline which do not require connectivity, we are also supporting the networks. So let's say you go out and buy something, you just tap your card on a terminal or phone, the other transaction time which is usually is expected around five to 10 seconds, in other cases up to 30 seconds, it comes down to a second or so.

GROWTH FACTORS

Our POS device, commercial over the shelf device use our online system rail and then we have for all ecommerce players and they have an element of home delivery wherein our app gets used. So if you have the home delivery part, then how to get our app gets used for the purpose of the delivery. All the manufacturers sell or update their product through stores, their online stores are driven by our e-commerce payment gateway offering.

GTM STRATEGY

Our machines are not simply machines, they are the enablers. We have apps into it and our back end system integrates with multiple acquiring banks, issuing banks, wallet players, UPI players, manufacturers for our signature product called Plutus Smart.

Our simple focus is to keep building new products, get the products that our merchant needs and we should be a partner to all merchant commerce. We are focused on solving problems for our merchants, customers, keep strengthening this app ecosystem and applications on the machines, bringing new things.

CYBERSECURITY POST COVID-19: ENSURING SAFE RETURN TO WORK

NEELESH KRIPALANI
Sr. VP & Head - Center of Excellence, Clover Infotech

The COVID-19 pandemic has created many challenges for businesses across the globe. At first, it was employees working from home and the cyber risks arising from the same. But now as we adapt to the 'new normal', many people are looking to make the transition back to office and there are new set of challenges to ensure safe return to work. The relaxation of stay-at-home orders and work restrictions are going to result in additional cybersecurity concerns which arise from the rapid reintegration of remote workers.

As there was a sudden switch to remote working style, there is an increased reliance on personal devices (such as personal computers, USB drives and other peripheral devices) for office related work. If any of these personal devices are compromised due to lack of security measures, then they can pose a serious threat to an organization's infrastructure as soon as they are connected to the internal network.

The new work-from-home world has poked countless holes in security perimeters. In the new normal, organizations and especially CISOs need to remain vigilant to various forms of risks and vulnerabilities that may appear once employees start returning to workplace. Some office-bound reflexes may have relaxed while working from home which can provide an opportunity to hackers to breach into the organization's network.

Thus, while the health of your employees must be the top priority while planning the return to work, you must also give due importance to the cybersecurity aspect to safeguard the organization's systems and data.

ANAND AND ANAND PLANS TO IMPLEMENT AND ENHANCE CAPABILITY ON SECURITY APPROACH

SUBROTO PANDA
Chief Information Officer, Information Technology Group, Anand and Anand

KEY PRIORITIES OF 2020

In our organizations, the digital workplace toolkit is broadly defined in eight categories to sustain the ways in which you communicate, collaborate, connect, and deliver day-to-day services. Too often, organizations implement these tools in silos without the benefit of a holistic digital workplace strategy.

Over the time we have developed our own capabilities for the design and deployment of future-ready IT systems that can flex as needed for innovation. Learn to use them to quickly reorient our operations while retaining the quality of user experience that our clients and members expect.

For example, our lawyers and members can reconfigure our client's engagement systems as the market changes. Your CRM system can lead teams to think more creatively about identifying and approaching customers.

Analysis shows emerging technology poses major new security challenges. But most C-suite executives are underestimating the risk—an oversight that could have profound effects on both innovation and growth potential.

We have organized the IT operating model in this way which offers many benefits. They include enhanced business–IT alignment, the ability to deliver faster innovation and greater value, more effective investments, and a simplified vendor landscape.

We plan to implement and enhance our capability on security approach for future-ready with our detailed technology analysis on:

ARTIFICIAL INTELLIGENCE — AI presents a completely new attack surface, including expanded approaches for machine learning models.

5G — 5G features such as virtualization, hyper-accurate location tracking and increased volume and speed of the network are escalating security challenges.

QUANTUM — This new computing paradigm presents numerous threats to organizations and data. Discover ways to safeguard against novel attack vectors, secure "trans pilers" and prepare now for post-Quantum cryptography.

EXTENDED REALITY — A variety of XR modalities present related vulnerabilities, especially when XR content is transferred over the cloud and AI recognition capabilities are on the cloud-as-a-service.

COMBINING BREAKTHROUGH & FUSION APPROACH

In a world where the old maxim "one technology-one industry" no longer applies, a singular breakthrough strategy is inadequate; Legal firms/companies need to include both the breakthrough and fusion approaches in their technology strategies.

First, the market drives the R&D agenda, not the other way around. If the customer wants a cheaper, smaller, and more reliable numerical controller for a machine tool, then that is the starting point for setting up R&D projects—not what the technologist has produced in the lab. Developing such a market-driven approach begins with demand articulation.

Second, companies need intelligence-gathering capabilities to keep tabs on technology developments both inside and outside the industry. Good surveillance goes beyond formal efforts, such as monitoring patent applications around the world. All employees, from senior managers to frontline workers, should be part of the collection and dissemination process as active receivers.

Third, technology fusion grows out of long-term R&D ties with a variety of companies across many different industries. Investment in research consortia, joint ventures, and partnerships goes beyond tokenism. Even though the risk of participation in many of these R&D ventures is high, the risk of nonparticipation is often much higher. Therefore, management must accept that it cannot evaluate each research investment on a short-term financial basis.

As enterprise becomes more and more data-driven, the need for quality data for law firm becomes essential. To this end, the race is on to enrich, remediate, and deduplicate enterprise data. Existing approaches rely either on human judgments about individual data points or on hard-and-fast rules that apply to entire data sets; in developing a new Data Labeling Workbench, we look forward to create a lightweight tool to significantly enhance and accelerate these data augmentation efforts. The Labeling Workbench uses AI techniques to provide a means for human experts to convey their knowledge in an efficient way and iteratively refine the resulting augmentations.

Fusion will play an increasingly important role in product development efforts in the future as more and more companies integrate it into their overall technology strategies.

CYBER SECURITY

One of the most immediate changes caused by COVID-19 for attorneys is the unprecedented number of attorneys working remotely. Outside law firms have, almost overnight, mobilized a remote work force throughout the country (and globally as well) of attorneys and support staff. Collaboration tools, like web-based videoconferencing platforms, have become key elements of many attorneys' work processes. The integration of these tools is unlikely to go away, even as attorneys return to the physical workspace.

Further, many courts have embraced technology in unprecedented ways. Judicial hearings via videoconference or teleconference are now commonplace, and judges are becoming increasingly comfortable with using technology to conduct court business and ensure that cases are moving forward. In the alternative dispute resolution arena, many mediators, arbitrators, and neutrals have wholeheartedly embraced technology and conducted mediations and hearings through videoconferencing tech.

Moreover, the practical effect of the economic downturn has meant that legal consumers are interested in identifying ways to lower legal cost. As a means to deliver value and drive efficiencies, lawyers and law firms should strongly consider remaining nimble and open to tools already available (and rapidly developing) that automate certain legal services, such as responding to complaints and discovery as well as automation of document review and other services traditionally performed by attorneys. When scaled, these tools can drastically reduce the cost of services provided by outside counsel and drive significant cost savings to clients.

The changes caused to the legal profession by the coronavirus pandemic are unlikely to be short term.

The sudden embrace of new technology has led to cybersecurity risks for law firms and employees working remotely. As organizations we should embrace cybersecurity and data privacy best practices to avoid data breaches and any compromise of internal or client data. For example, law firms must ensure that data is encrypted and that access to encrypted data is tightly controlled. Contracts with tech vendors should be closely reviewed to confirm that they contain terms with sufficient data protection protocols. With respect to videoconferencing, simple steps can minimize the risk of intrusion (or conference bombing), like separately sending conference meeting identification numbers and passwords or turning on participant identification features. Further, virtual private network (VPN) use is advisable if possible; a VPN provides a direct connection to an organization's normal computer applications as if an employee were directly connected to the organization's computer network. Moreover, reminders to personnel of phishing risks and firm policies regarding malware are important and should be refreshed regularly during a remote work environment.

"DIGITAL TRANSFORMATION HAS A HOLISTIC IMPACT ON THE BUSINESS"

SUNIL GUBRANI
Head – IT,
RAL Group

KEY PRIORITIES OF 2020

While the cloud, cyber security and analytics will always be important, in 2020 we are looking into the bigger picture at ways to better integrate technology and enable greater success -

1: Understanding the business as a whole
2: Technology enabling communication and collaboration
3: Better and more consistent training
4: Implementing AI

COMBINING BREAKTHROUGH & FUSION APPROACH

Digital transformation has a holistic impact on the business. It impacts almost every aspect of the operations, including people, their skills, work capacities and culture. Additionally, it also involves the processes that include tasks, methods, approaches and workflows. The one thing it doesn't change is the core values. Rather, it is about creating a well-connected workplace culture and attaining digital transformation tools that support the strategy and goals. The outcome of having digital transformation is to define strategic route, risk craving and budget, rate of change, agility, and technology enablement.

CYBER SECURITY

Cyber security is important because it encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries.

Cyber threats can come from any level of organization. Staff should be educated about simple social engineering scams like phishing and more sophisticated cyber security attacks like ransomware (think WannaCry) or other malware designed to steal intellectual property or personal data.

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether an individual, small business or large multinational, one relies on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cyber security threats that did not exist a few decades ago. We need to understand the difference between cyber security and information security, even though the skillsets are becoming more similar.

> "Over the last few years, most discussions about the next year's Digital Transformation trends had begun to feel a bit repetitive: Cloud, Edge Compute, the IoT, AR. It always seemed like the same chairs being rearranged around the same old room. 2020 will be a departure from that. While the same core technologies that dominated these discussions will continue to be foundational to our collective digital transformation journey, 2020 will be defined by a fresh new class of technologies ready to graduate to the sidelines to center stage."

"COMPANIES SHOULD TAKE A POSITIVE APPROACH ON TECHNOLOGY TRENDS AND ALSO MAKE THINGS ACCORDINGLY KEEPING COMPLIANCE IN MIND"

KEY PRIORITIES OF 2020

We are already in the process of implementing new security tools and also started VAPT on our apps on a regular basis.

COMBINING BREAKTHROUGH & FUSION APPROACH

Companies should take a positive approach on technology trends and also make things accordingly keeping compliance in mind.

DEEPAK KALAMBKAR
AVP Infrastructure
SAFEXPAY

> "We will be launching our app in the market and for this we are in a process of doing the compliance checking for the same."

RELAXO FOOTWEARS PLANNING TO TAKE THE SECURITY POSTURE TO THE NEXT LEVEL

KEY PRIORITIES OF 2020

We have plans to improve the security posture of the organization from current level to next level.

CYBER SECURITY

We have plans to spread awareness of cyber security in the organisation.

AJAY TYAGI
DY. GM-IT,
Relaxo Footwears

> "We have plans to focus on digital transformation in the current year."