

ITNEXT

FOR THE NEXT GENERATION OF CIOs

THE FAST CHANGING PROFILE OF CYBER SECURITY RISK

Why CISOs
need a different
kind of planning to
handle it?

LAUNCHING



Here is your chance to become a Digit certified tech influencer

Benefits of Digit Squad Member



Launch your own tech channel on Digit.in



Become a Digit Certified tech influencer

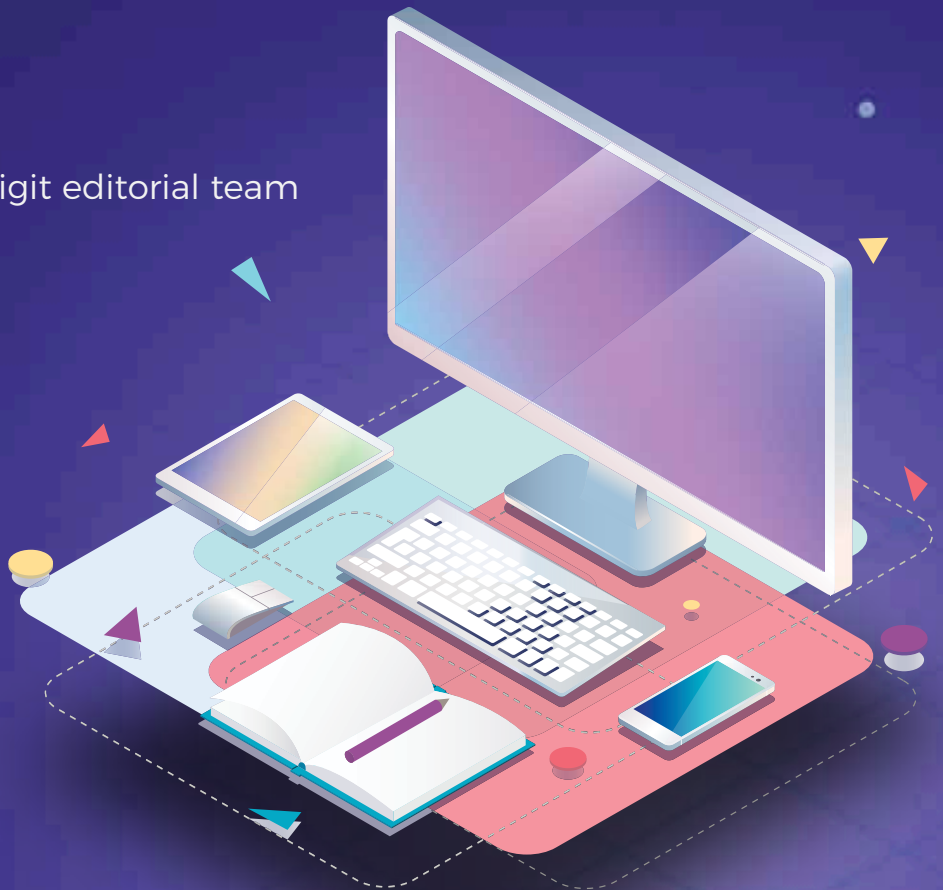


Engage with digit editorial team



Make money

Apply now by scanning the QR code



www.digit.in/digit-squad/apply.html

For CISOs, integration is the way forward



Governance,
communication,
collaboration,
risk management
practices...they sound
very different from
identity management,
authentication,
endpoint protection,
SIEM...

Shyamanuja Das

Traditionally, corporate IT departments have been the custodians of anything to do with data. The top executives were dependent on them to get data, analyze it, and even to make sense of it.

As the importance of data grew in the business, businesses started hiring specialist data scientists. Today, it is an established practice for large and medium organizations to have a separate data team.

Ditto for Chief Digital Officers. When the posts were envisaged, the IT executives were the top claimants for them, with some challenge from the marketers who thought they understood digital media really well. In hindsight, we see, it is mostly core business people who occupy those roles.

Turn to information security. As the profile of cyber risks grows in organizations—cyber risks being counted among top five business risks (see the cover story)—there are similar apprehensions. Will it be taken away from the people who have traditionally handled it? Will trained risk professionals with business background take over?

Nah, it is not happening. Most research show that CIOs and CISOs are still the top custodians and decision makers when it comes to cybersecurity. The cover story in this issue highlights some of those.

What explains the trend? Highly specialized nature of jobs, lack of manpower who can do that effectively? Many reasons, let us keep that discussion for another day.

What we have highlighted in this issue's cover story is—what comes after this seemingly good news?

It is tough—if not bad—news. The CISOs and CIOs get to keep this responsibility with them for the time being, not because they seem to be the perfect choice, but because they are perceived to be the best choice among all available options.

They have to go a long way to be able to do that effectively. What is needed is a change in attitude and a change in planning. We focus here on the second part. Changing attitude is a big challenge and we promise to do a research-based story on that in the near future.

Even when it comes to planning, you can clearly see it is not so much about tech. Governance, communication, collaboration, risk management practices—these are some of the suggested focus areas. They sound very different from identity management, authentication, endpoint protection, SIEM...

One obvious question is: When the CISO today is expected to ensure compliance to different regulatory requirements and some companies are even toying with the idea of making CISOs the Data Protection Officers (DPO) as required by the upcoming personal data protection legislation, how can they manage all these?

From all that we have seen in business over the years, we can find a clue. And that is: not to see these as separate tasks but create an integrated approach combining tools, technologies, practices and management. Doing that is not rocket science, but stepping two steps backwards from day-to-day fire-fighting to see things in broader perspective and then think of a holistic solution is the real challenge. ■

Content

■ COVER STORY | PAGE 06



THE FAST CHANGING PROFILE OF CYBER SECURITY RISK

Why CISOs
need a different
kind of planning to
handle it?

FOR THE LATEST
TECHNOLOGY
UPDATES GO TO

IT NEXT.IN



FACEBOOK
[WWW.FACEBOOK.COM/ITNEXT9.9](http://www.facebook.com/ITNEXT9.9)



TWITTER
[HTTP://TWITTER.COM/ITNEXT_](http://twitter.com/ITNEXT_)



LINKEDIN
[HTTPS://IN.LINKEDIN.COM/PUB/IT-NEXT/68/717/301](https://in.linkedin.com/pub/IT-NEXT/68/717/301)

MANAGEMENT

Managing Director: Dr Pramath Raj Sinha
Printer & Publisher: Vikas Gupta

EDITORIAL

Managing Editor: Shyamanuja Das
Assistant Manager - Content: Dipanjan Mitra

DESIGN

Sr. Art Director: Anil VK
Art Director: Shokeen Saifi
Visualiser: NV Baiju
Lead UI/UX Designer: Shri Hari Tiwari

SALES & MARKETING

Director - Community Engagement:
Mahantesh Godi (+91 98804 36623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Head - Community Engagement:
Vivek Pandey (+91 9871498703)
Community Manager - B2B Tech: Megha Bhardwaj
Community Manager - B2B Tech: Renuka Deopa

Regional Sales Managers

North: Deepak Sharma (+91 98117 91110)
South: BN Raghavendra (+91 98453 81683)
West: Shankar Adaviyar (+91 9323998881)

Ad Co-ordination/Scheduling: Kishan Singh

PRODUCTION & LOGISTICS

Manager - Operations: Rakesh Upadhyay
Asst. Manager - Logistics: Vijay Menon
Executive - Logistics: Nilesh Shiravadekar
Logistics: MP Singh & Mohd. Ansari
Manager - Events: Naveen Kumar

OFFICE ADDRESS

9.9 Group Pvt. Ltd.

(Formerly known as Nine Dot Nine
Mediaworx Pvt. Ltd.)

121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091

Published, Printed and Owned by 9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt.
Ltd.) Published and printed on their behalf by
Vikas Gupta. Published at 121, Patparganj,
Mayur Vihar, Phase - I, Near Mandir Masjid,
Delhi-110091, India. Printed at Tara Art Printers Pvt
Ltd., A-46-47, Sector-5,
NOIDA (U.P.) 201301.

Editor: Vikas Gupta



© ALL RIGHTS RESERVED: REPRODUCTION IN WHOLE
OR IN PART WITHOUT WRITTEN PERMISSION FROM 9.9
GROUP PVT. LTD. (FORMERLY KNOWN AS NINE DOT NINE
MEDIWORX PVT. LTD.) IS PROHIBITED.



■ INTERVIEW | PAGE 12-13
"Tech Leaders
Should Focus On
Improving Customer
Experiences"



■ INSIGHT | PAGE 15-17
Importance Of IoT
In Manufacturing
Sector



■ INSIGHT | PAGE 18-19
Healthcare - A
Vulnerable Sector For
Cybercrimes



■ INSIGHT | PAGE 22-23
How CIO Can
Become The
Boardroom
Influencer



■ INSIGHT | PAGE 30-31
Effective Security
Performance
Management Need
Of The Hour: Study



Cover Design:
ANIL VK



Please recycle this magazine
and remove inserts before
recycling



For the love of the sea and its mysteries

Taking The Plunge

NEXT100 Winner 2018 **Harish Shankar**, IT Security Manager, Schneider Electric, shares his passion for scuba diving...

Scuba diving has become a passionate activity for me in the past few years. My college days were closely associated with the sea, as my college is located on the seashore. I like to keep fish as pet, and when I was younger, I reared hundreds of them in mud tanks as a hobby. I used to visualize the life of fish under water while I watched them in my big mud tank. I didn't realize then that my proximity to sea and fondness for fish will trigger a passion in the future.

Scuba diving started as one of the activities during a vacation in western Karnataka. Since I was a good swimmer and swam in rivers, I was confident that I could do it. There was a group of people who had registered for diving. We began practicing in the pool the

previous day and learned how to communicate under water using signs and safety techniques.

On the day of diving, we were taken to the dive sight. It was my turn after couple of my dive mates. I was accompanied by an instructor as this was my first diving exercise. After gearing up, I was pushed into the water. I felt very uncomfortable and scared with the diving suits and equipment. I started giving up and wanted to come back to the boat. Thoughts were running rapidly in my mind. I told to myself that if I come out of my comfort zone, I will have a beautiful experience – fish in the deep sea – what I had long imagined. Then I started thinking “Am I taking risk or just overthinking?”. By then, the instructor held my hand and it gave assurance of my safety. We eased up a little over the water and started our journey under the sea.

I have performed several dives. Each time I dive, I experience something new. Currently, I am planning to obtain Diver's C-Card (Certification Card) which is recognized globally and can be used anywhere in the world. ■

As told to Dipanjan Mitra, Team ITNEXT



Harish Shankar

Harish Shankar is IT Security Manager at Schneider Electric. He is NEXT100 Winner 2018. Earlier, he had worked in companies like Cisco and Cognizant. He completed his

Snapshot

BTech in IT from Pondicherry University. Some of his key certifications include ITILv3 Foundation from EXIN and Certified Ethical Hacker (CEH) from EC Council.

Keeping Up With Technology

NEXT100 Winner 2018 **Sanjay Bakshi**, Senior Program Manager - Database Services, Safexpress, shares his passion for working with computer hardware...

I still remember that day: Sometime in late 1980s, about 30 years ago, when computers were first introduced as a subject in our school. To start with, we got one IBM PC-XT machine with DOS operating system which used the 5.25 inch floppy disk to boot & had a 14" CRT mono monitor for display. Throughout the week, we used to wait for the computer period and then await our turn on the machine as there were over 30 students in the class, mostly just to get a chance to play a round of Pac-Man!

Time passed and as soon as I started earning, I was saving money to be able to afford one; shortly, I was learning the ropes with a PC of my own: An Intel Pentium 200 MMX processor with 16 MB RAM, 2GB HDD, a 2MB Video Card & a 15" Colour Monitor.

Having always been a "hands on" person and never the one to shy away from disassembling/assembling stuff; without realizing it, my romance with computers/smart devices/automation devices/technology had started. It took me some time, but I finally decided to make a career in the upcoming software industry.

Many years have passed and true to "Moore's law", the hardware specifications and advancements have kept up pace. Even today, a configuration considered top of the line 18-24 months back, soon starts looking obsolete.

Hence, the need to upgrade frequently and also the chance to handle the technological hardware up close. Being a senior IT professional with a leading logistics company means that you have minimal free time available and balancing various facets of life like bonding with family and friends, following your passions, hobbies, travel, leisure, etc., can be very challenging.

Hence, it was a joy to discover that both my son, Sanjeet, a well-informed 14-year-old and daughter, Saanvi, 7 years old, excited to



A family that 'hardwares' together stays together

prepare for her first Cyber Olympiad, shared my passion for technology and exploring how things work. Aptly supported by my wife, it has become almost a regular ritual to get together on holidays (mostly Sundays only) and work on some project.

One of the recent projects completed was to assemble a new PC from scratch with the latest available configuration. It also involved installing an AMD processor and using a SSD disk which were a "first time" for us. Another one was to upgrade the processor of an old machine from an Intel core 2 duo to an Intel quad core processor and use the freshly rejuvenated system as the media center at home. Many projects are lined up for the near revolve around home automation using Google Home/Alexa and even an AI video bell.

Technologically speaking, "we are living in the most exciting times ever" since the advancements in hardware and software are feeding each other to the next level without ever becoming a bottleneck for the other. With the AI/ML space growing by leaps and bounds, it can only get better! ■

As told to Dipanjan Mitra, Team ITNEXT

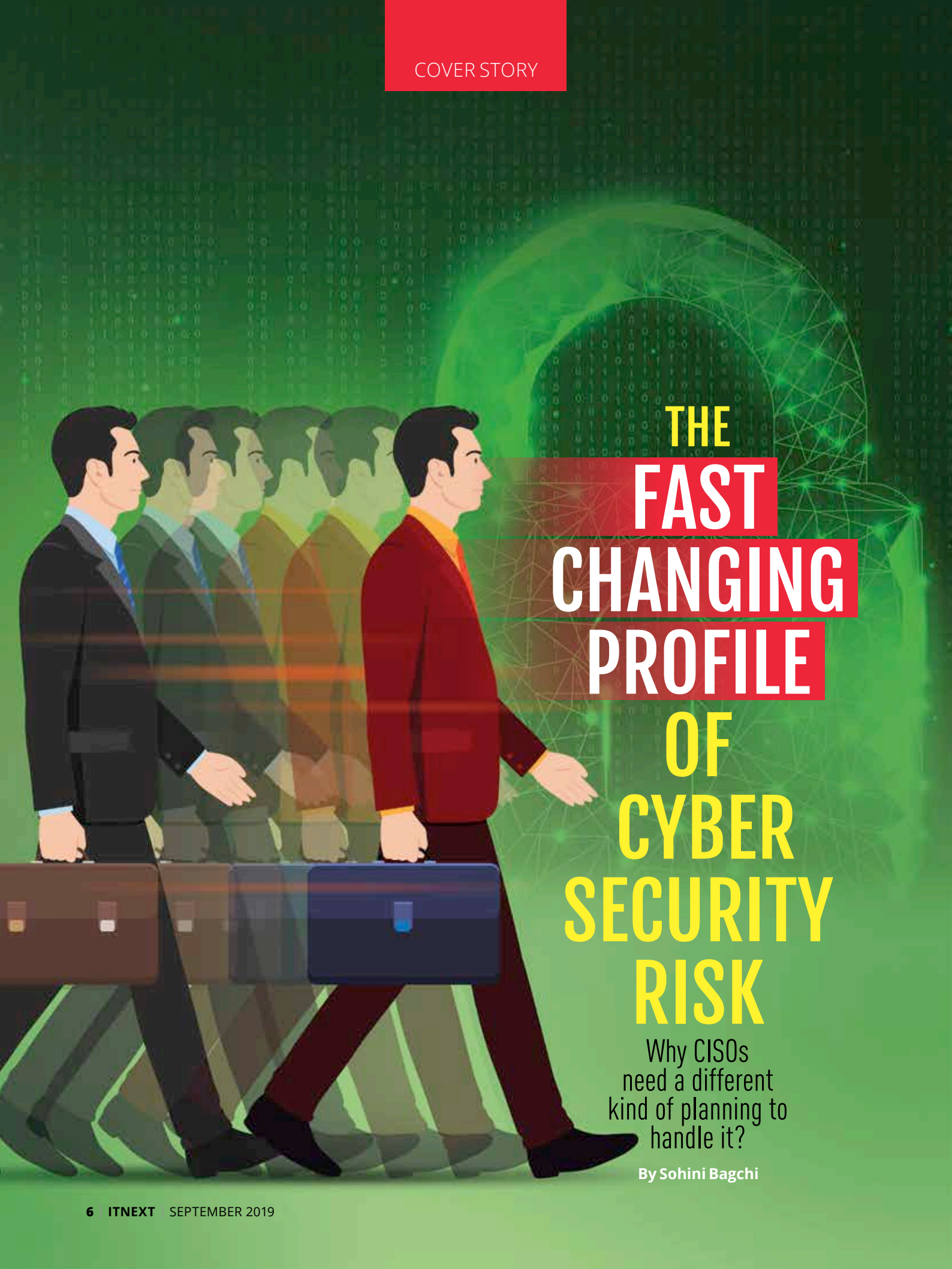


Sanjay Bakshi

Sanjay Bakshi is Senior Program Manager - Database Services, Safexpress. He is NEXT100 Winner 2018. Bakshi has earlier worked in companies like Vinculum Solutions and Tomax Corpo-

ration. He has done his PG Diploma in Personnel Management from Annamalai University and Bachelor's Degree from Kakatiya University. He is Oracle Certified Professional (OCP).

Snapshot



THE FAST CHANGING PROFILE OF CYBER SECURITY RISK

Why CISOs
need a different
kind of planning to
handle it?

By Sohini Bagchi

The annual Global Risk Report (GRR) of Geneva-based global think tank, the World Economic Forum (WEF), based on its Global Risk Perception Survey, is arguably the most important current risk assessment statement at a global level. This report hugely influences the risk planning strategy of global businesses, financial institutions and world governments.

In this year's GRR, two cyber security risks—data fraud/theft and cyberattacks—were identified as two of the five most likely risks for 2019, next only to extreme weather events, future of climate change mitigation & adaptation and natural disaster—and ahead of such risks as man-made environmental disasters, large-scale involuntary migration, biodiversity loss and ecosystem collapse, water crises and asset bubbles in a major economy.

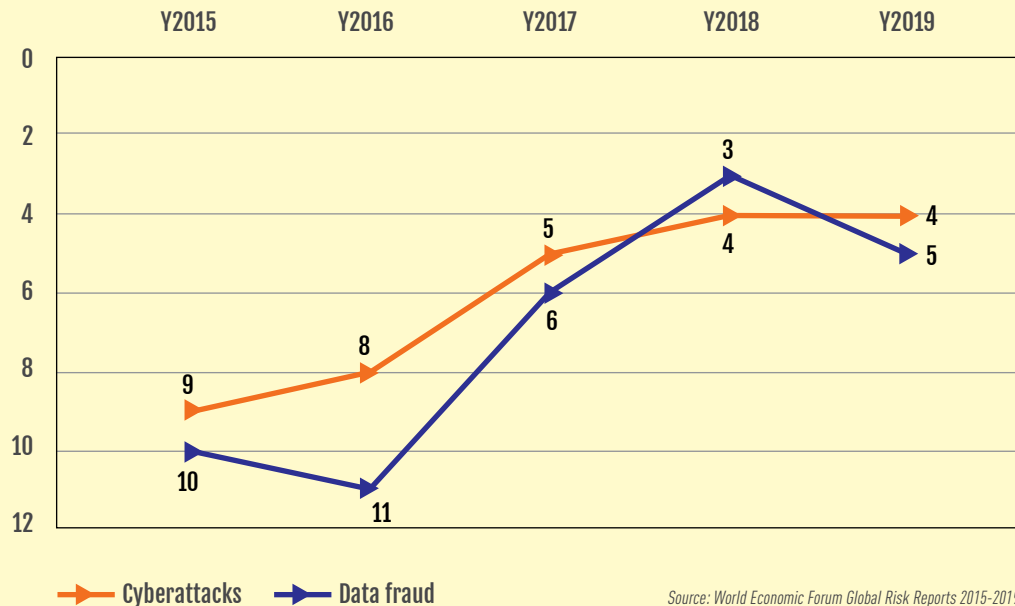
The WEF GRR also ranks the risks in terms of impact. Cyberattacks was ranked as the seventh most impactful risk, along with such risks as weapons of mass destruction, extreme weather events, future of climate change mitigation & adaptation, and natural disasters.

According to the GRR 2019, a large majority of respondents expected increased risks in 2019 of cyberattacks leading to theft of money and data (82%) and disruption of operations (80%). Around two-thirds of respondents expect the risks associated with fake news and identity theft to increase in 2019, while three-fifths said the same about loss of privacy to companies and governments.

The 2019 report is not an isolated example of a GRR counting cyber risks among the top global risks. The likelihood of cyber risks has consistently gone up in the WEF annual surveys. In 2015, data fraud ranked as the 9th most likely global risk in the year's GRR. It has consistently risen as a risk to rank as the 4th most likely this year. Similarly, just three years back—in 2016, cyberattacks were seen as the 11th most likely risk, which is today ranked as the fifth most likely. In short, the high

RISING PROFILE OF CYBER RISKS

Rank of cyber risks in most likely global risks identified by WEF



likelihood factors associated with cyber risks are not an accidental one-off phenomenon; its rise as a global risk has been gradual and consistent.

Cyber risk as a corporate risk

While the GRR tries to assess the risk from the point of view of a broader global community—that includes governments, multilateral agencies and financial institutions—how serious are the businesses about cyber risks.

A survey conducted in 2018 by insurance broking and risk management company Marsh and IT major Microsoft shows how companies see the seriousness of cyber risk. According to the Marsh-Microsoft Cyber Perception Survey, nearly two-thirds of survey respondents see cyber risk being among their organization's top five risk management priorities. That is roughly double the percentage who rated cyber that high in a survey Marsh conducted in 2016. From the companies that the research covered, 56% ranked cyber security risks among their top five risks and a small but significant number—6% of all companies—ranked it as the biggest risk!

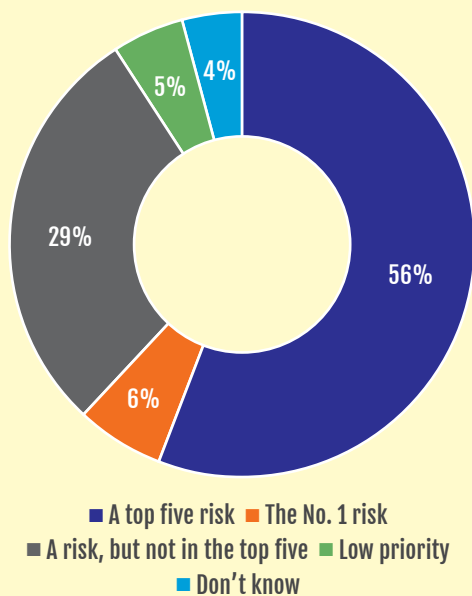
No wonder, they have started quantifying the financial cost of major cyber incidents. From among the USD 1 billion dollar-plus companies, as many as 42% estimate the worst potential value of financial loss in case of an incident to be more than USD 50 million, out of which two-third estimate the loss to be more than USD 100 million.

A new Aon report puts a number to the magnitude of the aggregate losses. It estimates annual global cyber losses are expected to hit USD 6 trillion by 2021, with cybersecurity spending projected to exceed a total of USD 1 trillion for the five years leading up to 2021.

The report, 'Prepare for the unexpected: Safeguarding value in the era of cyber risk', notes that while the immediate costs of a cyberattack can be significant, damages to a business's reputation could cost just as much or even more in the long-term.

According to a research published in June this year by ESI ThoughtLab, on an average, annual losses from cyberattacks grew to USD 4.7 million last year—with more than one in 10 companies losing more than USD 10 million. That amount equates to an average of 0.114% of revenue across all firms surveyed.

HOW DO COMPANIES SEE CYBER RISK?



Source: Marsh-Microsoft Cyber Risk Perception Survey 2018

Are cyber risks too serious to be left to the techies?

As we have seen in many cases—including the roll-out of digital strategies in organizations and transformation to data-driven business models—when something becomes too important, people turn to newer more specialized workforce or push the responsibility upwards.

Is cyber security too becoming too important to be left to the custodians of technology—the IT department?

Answer is a clear and resounding No. Maybe because of the specializations involved as well as lack of enough manpower, organizations are not taking away cyber security responsibility from the IT guys—the CIOs and CISOs, even among the largest of organizations.

According to the Marsh-Microsoft survey, as much as 77% of respondents from more than USD 5 billion plus companies said IT is the primary owner and decision maker for cyber risk management in their organization. For companies between USD 1 billion and USD 5 billion in revenue, that number rises significantly to 83%.

What it means is:

1. Organizations have begun to recognize the seriousness of cyber risks and have even started assessing it financially.
2. They have most decisively shown that they will continue to expect the management of that risk from their IT guys—the CIOs and CISOs.

The CISO challenges

The rising profile of cyber risk is significantly due to the rise in complexity and sophistication of cyber risks.

“Today, attackers have reached a certain level of maturity and efficiency. They are taking advantage of the increased value and vulnerability of online targets that is resulting in a dramatic increase in attack frequency, complexity and size,” says Sheril Jose, Head - Cyber Security at Pune-based Emcure Pharmaceuticals.

Vijay Radhakrishnan, CISO of Mahindra & Mahindra Financial Services adds to this explaining, “New threats are comprehensive, intelligent and are highly stealthy. While threat assessment, monitoring and attack curtailment have gone in the direction of big data analytics, ML, AI and blockchain way, hackers work in similar war filed and are well financed to do so. It’s almost cyber militancy which is managed on a daily basis.”

How significant is the challenge for India? The average value of loss reported by the ESI ThoughtLab research quoted above across countries shows that at an average of more than USD 6.5 million, the value is second highest for Indian companies, closely behind the average value of loss reported for German companies and significantly higher than the average loss of companies in the US, China, France, the UK and Japan.

Quick Heal’s ‘Annual Threat Report 2019’ gives a more detailed view of Indian cyber security landscape. It states that most CISOs in India are grappling with newer issues, such as cryptojacking, ransomware and threats to mobile devices that were unheard even five years ago. With the increased use of new technologies, such as Artificial Intelligence (AI), Blockchain and the Internet of Things (IoT) in the enterprise, as well as increased popularity of digital transactions in recent years, CIO/CISOs must adopt innovative techniques to manage the escalated threats.

However, these are not problems specific to India, as the country is part of the connected global ecosystem, where advanced persistent DDoS

campaigns are now the norm. Also global growth of IoT devices is becoming great breeding ground for hackers to enslave more and more devices. To further complicate things, attackers are taking advantage of SSL-encrypted traffic to camouflage their attacks, making it hard to determine malicious versus legitimate traffic.

While the average cost of breaches is humongous, the most challenging part is budget and skill constraints. There's also lack of support from senior management, preventing CISOs from implementing a cohesive cybersecurity strategy.

"The CISO has to ensure that controls are implemented in the right manner within the organization and they are based on the results of risk assessment and not on the decisions of functions," says Meetali Sharma, Corporate Risk, Compliance & Security Leader at SDG Software India.

"Also with so many products in the market, one of the key security challenges is to ensure that you pick the right tools/technologies for your organization based on the need of the organization and not just because it is a fancy tool and gives nice dashboards," she adds.

Gearing up against cybercrime

To fight against cybercriminals, firms are investing more in their cybersecurity budgets from what they did in the past. CISOs now have a huge responsibility to continually assess the security tools and processes they've put in place in their organizations to prevent a breach or cyber attack. To be ahead of the game, CISOs are continuously reviewing their cybersecurity processes and practices to ensure that adequate and effective systems are in place.

Integrating security and business risks management

A recently released 'Cisco 2019 CISO Benchmark Study' observes that CISOs are modifying and expanding their security strategies to address new and emerging security threats. Nearly half of the survey's respondents (47%) report that they are now using outcome-based objectives to focus on their security spending. For instance, many companies are investing in threat intelligence programs that are helping them identify, prevent and respond to these threats through informed decisions.

Wendy Nather, director of advisory CISOs at Duo Security, a Cisco unit, mentions in the report that CISOs are making sure that the results are

tangible. "In terms of strategy, the vast majority of organizations (94%) are practicing incident response at least once a year; 61% are doing it at least every six months. "These exercise drills are helping enterprises develop the skills they need to face evolving security threats," she says.

It is important to integrate security and business risk management. "Cybersecurity is not an isolated aspect of an organization. Its impact goes beyond IT and can have serious legal and reputational implications. IT security, then, should not be detached from the wider business risk management strategy," says Makarand Sawant, Senior General Manager - IT, Deepak Fertilisers and Petrochemicals Corporations Limited.

Focus on better IT governance

There is also increased focus on better IT governance, as new challenges stemming from the increasingly complex regulatory environment, including new regulations (like GDPR and Indian Data Protection Act) are evolving, and enhancements to existing regulations are coming up, thereby forcing organizations to comply with it.

"It is very important to carefully keep monitoring your controls and harmonizing them. A new control should not be implemented to meet a new regulatory requirement, rather, one should try to reuse and enhance an existing control based on the changing needs. An organization's security framework should be extensible enough to accommodate such changes in this agile regulatory environment," Sharma says.

A 2018 ISACA report found that IT governance is essential to strong business performance and is now a board-level priority. It recommends CISO/ CIOs and boards should define an appropriate set of security policies and associated procedures and security architectures for each business risk.

Greater collaboration and communication

Gap in communication is a major barrier in the direction of effective security. Despite having a solid security framework in place, lack of collaboration at the C-suite has been found to jeopardize cybersecurity in organizations. A recent report by Accenture found only 40% of the CISOs surveyed said that they always confer with business-unit managers to understand the business before proposing a security approach, pointing at a shortage of ongoing communication and lack of trust.

"A better engagement between CEOs, board members, and CISOs or CIOs will result in a fine-tuned and effective cyber risk mitigation strategy," says Sawant.

"CISOs and CIOs need to work with their C-suite colleagues and board directors to bring governance practices into the digital age. Now that boards are accepting that cyber risk management and regulations require their oversight as much as any other business risk, it is time security leaders become more vocal about their task at hand," agrees Jose.

"In such a scenario, security leaders need to keep abreast of the latest threats and prepare for the outcome of every strategy. Security should in fact be the board's top priority and the management should take it very seriously. Adoption of best in grade technology is important for every organization. CIO/CISO needs to constantly communicate the same to the C-suite," Radhakrishnan of Mahindra & Mahindra Financial Services says.

The Marsh-Microsoft survey found 45% of risk and technology executives saying that they send information on cyber investment initiatives to board members, while only 18% directors say they receive it. That is a big communication gap.

Training and enablement

The impact of the talent and skills shortage is also profound within today's organizations. This shortage can prohibit strategic goals and leave businesses at risk. A Forbes Insights and Fortinet survey, titled 'Making Tough Choices: How CISOs Manage Escalating Threats and Limited Resources', states, security leaders are currently allocating an average of 36% of their security budget on response. However, in an ideal world, they would shift their resources from prevention to bolster detection and response. It is in this context that CISOs are paying more attention to educating their own employees on best practices and building cybersecurity awareness in order to prevent and reduce internal threats.

As per the '2019 Verizon Breach Investigations Report', about 52% breaches featured hacking and close to 34% attacks involved inside actors. In order to best respond to threats, security leaders must focus on talent, team training, and strategy implementation.

"Since a lot of ransomware and phishing attacks are planned attacks and the root cause is employees in most of the cases, it is very important to ensure that adequate education and awareness is given to employees to make them a part of all the information security initiatives. Each employee should be a co-owner of security within the organization and should understand its importance," recommends Sharma.

The road to confidence

Top priorities for many CISOs in the coming year will be to enable an enterprise-wide holistic security approach and hire more cybersecurity staff, as the Fortinet report suggests. In 2020, 14% of CISOs will dedicate priority funding to adding more security personnel to their teams. Additionally, over the course of the next five years, 16% of CISOs aim to develop a culture of security throughout their entire enterprise.

Despite taking tangible steps to reduce cybersecurity risks, cybersecurity continues to be an ever-evolving struggle for organizations. Sophos in its research report, titled 'The Impossible Puzzle of Cybersecurity', clarifies that there are 'always' some security holes not being plugged and it is here that CISOs need to pay greater attention. For example, the report explains, an up-to-date malware signature list won't stop attackers hijacking your accounts, while rock-solid authentication won't help if you're not protecting your computers from ransomware.

"Good cybersecurity demands defense in depth and proper risk assessment so that you can protect your weakest spots from attack first," says Chester Wisniewski, principal research scientist at Sophos.

At the same time, companies are facing attacks via multiple channels, including email, web and app-based platforms, among others. Software vulnerabilities and unauthorized USB sticks or other external devices were also common attack vectors. Sometimes, organizations are also not aware that their networks were compromised.

Good news is, Wisniewski believes, seasoned CISOs know that a good digital defense is not enough, so they are building a multilayered approach that includes stronger investment in people and process. Recognizing that some hackers will inevitably find a way in, CISOs are recalibrating their cybersecurity budgets to focus more on remediation. And many CISOs believe that their investments are already paying off.

To stay ahead of the game, companies need to stay vigilant everywhere, since attackers are relentless in exploiting weaknesses. With limited budgets, and cyber risks mushrooming, it is paramount that organizations understand the ROI of cybersecurity so that they invest in those efforts that will result in maximum outcome. By being prepared yet flexible and implementing new and innovative techniques, CISOs will enable a scalable defense fit to counter the breaches ahead of them. ■



“Tech Leaders Should Focus On Improving Customer Experiences”

Natasha Jethanandani, CTO of Kaleidofin illustrates what it takes to head the technology team at her organization and reflects on the changing role of IT leaders

By Sohini Bagchi

The role of the Chief Technology Officer (CTO) is drastically changing in recent years from a tech-centric role to one having leadership, vision and a more customer-centric approach. In an exclusive interaction, Natasha Jethanandani, CTO of Kaleidofin – a digital financial services platform that offers innovative investment solutions – reflects on the changing role of IT leaders in the industry. After stints at Google and Microsoft, Jethanandani explains what it takes to head the technology team at a fintech company, a sector that is increasingly relying on advanced technology innovation and customer-centricism.

Q How do you see the IT leader's role has changed over the years?

A Having spent close to 15 years in the sector, I believe one of the most important aspects that changed for technology leaders is the focus on building better customer experiences. Today, an increasing number of companies have a mobile-first approach, which leads to creating integrated interfaces and an end-to-end customer engagement experience. Understanding the target segment to build UX that resonates with them, along with creating a seamless backend that provides functionality in a performant and scaled way should now be the focus of any technology team.

Q What is the role you play in your organization? How do you draw inspiration to manage your day-to-day operations?

A Kaleidofin is a tech-led platform that provides integrated financial solutions to the under-banked. Our solutions are entirely online and accessible by customers through the Kaleidofin App. As a CTO, my responsibilities are divided into both building the customer facing

app as well as scaling the backend and automating processes to create a seamless experience.

The Kaleidofin business strategy and growth plans posed several challenges to us. First, Kaleidofin is a mass market product. We aim to get a minimum of a million customers over 2 years. The technology systems therefore had to be built to work with large volumes.

Second, our target segments are diverse, not just in their financial service needs, however, we wanted to make sure we offer customised services for each one of them. Our app today, creates a risk persona for each individual customer and suggests a solution based on the same.

My team members and I regularly interact with the agents who work with the customers as well as the customers to understand and make changes in our systems. In less than a year, we have seen many customers increase their saving capacity from INR 100-1000. The interactions and also the success ratio with customers keep us motivated about our work.

Q What were the lessons you learnt from your Microsoft and Google days?

A As technology professionals, it is imperative to experiment and learn each day and I believe that's one lesson that I carry back from my Google and Microsoft days. Microsoft and Google were undoubtedly amongst the best learning launch pads. Here each employee, irrespective of the number of years of experience is encouraged to come up with new ideas and question existing ones. The companies had an entrepreneurial culture. Every team was encouraged to initiate new projects and new ideas. However, the teams had to convince technical architects and business leaders internally about the value propositions of these projects. Working with incredibly smart people day in and day out was very motivating. I encourage my team constantly to debate and question

constantly. Within Kaleidofin, we keep track of new trends, platforms and what is going on in the industry and try to inculcate a continuous learning environment.

Q What's your view on the state of women CIO/CTOs in India? How do you support more women tech leaders in the workforce?

A As mentioned above, the role of a CTO /CIO is now becoming strategic in nature that has a direct impact on business. The choice of a CTO /CIO is entirely based on an individual's capability and commitment to work.

We have a gender agnostic approach at Kaleidofin. Having said that, our policies such as flexible work times, support for work life balance, etc, makes it an employee friendly place which encourages more women to work with us. Also, we are excited that we have a great set of women leaders – our CEO is a woman and we have strong women leaders in Product Management, Business Development and other teams as well.

Q What role does innovation play in IT? How do you ensure that your team makes enough time to innovate and create new business led IT tools?

A There are new technology advancements almost every day - across many areas including cloud platforms, AI/ML and at a device level. It is important for any technology team to not just keep abreast with the new developments but also incorporate them in their existing systems and processes.

At Kaleidofin, we strive to do this regularly. A good example is where we observed a business problem wherein customers KYCs were failing regularly due to poor quality pictures taken in the field. We immediately incorporated AI-based OCR technology into our mobile app to do text recognition on the pictures captured and prevent

poor quality pictures at the source itself. This had the advantage of catching issues real-time and also reduced operational costs significantly.

At Kaleidofin, we encourage our teammates to constantly research and learn from developments in the industry. We also invite experts and professionals from the industry to share their learning with us.

Q What technologies are you toying with or are likely to explore in the future?

A We are actively looking at technology that helps build scalable platforms using commodity hardware – architecture that uses microservices to create reliable and multi-tenant systems, building a high performant data pipeline that can be used for near real-time analytics.

We are looking at AI based technologies that can help with customer engagement – personalization, improved onboarding, improved communication using NLP techniques (voice recognition, chatbots), issue resolution that 'learns' customer needs (using multi channel customer service assistance). Also, customers are getting comfortable with voice-based tech (voice-to-text, text-to-speech) and we are exploring how to apply this along with a strong focus on vernacular. We are further using AI, OCR and computer vision techniques to move towards Robotic Process Automation (RPA) and machine learning and anomaly detection to prevent fraud.

Q What are your tips to future CIO/CTOs or IT leaders?

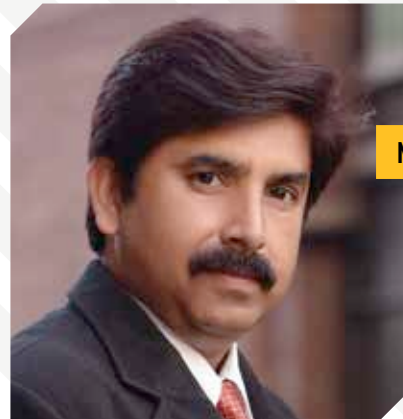
A The world of technology is today dynamic and constantly evolving. New platforms and developments in technology, AI and ML have a huge impact on business models. For any technology professional therefore, it is more important than ever before to set aside enough time to learn and evolve with the changes, take on leadership roles and new challenges.■

NEXT100 Winner Appointments


ARCHIE JACKSON

Archie Jackson has joined technology services and consulting firm, Incedo as Senior Director and Head of IT & IS.

Jackson, a NEXT100 winner in 2011, was with Genpact as AVP - IT and Information Security, prior to joining Incedo. He has also served in major IT services and consulting firms such as Capgemini and Steria.


MANORANJAN KUMAR

Manoranjan Kumar has joined Trident Group as CIO. He was NEXT100 Winner in 2012. Kumar was earlier

associated with Shree Cement and Kanoria Chemicals & Industries Limited in the same capacity. He had also undertaken various leadership and managerial positions at companies like Lanco Infratech, Samtel Color, Rockwell Automation and Dalmia Industries.

Kumar completed his MBA in MIS and Computer Sciences from XLRI - Jamshedpur, MSc in Computer Science from Pt. Ravishankar University and PG Diploma in Aligning IT Strategies with Business from Indian School of Business.


PRIYA DAR

Priya Dar has joined Amway as Head of Digital Strategy & Innovation. She is NEXT100 Winner 2016. Earlier, she

was associated with Godfrey Phillips India as CIO. She has also worked in different leadership and managerial capacities in companies like Indus Towers, IDT, Random Walk Computing, Capgemini, AT&T, Times of India and Nicot Systems.

Dar had completed a Certificate course in Digital Strategies for Business from Columbia Business School Executive Education and BE in Computer Science from University of Pune.


TEJAS MEHTA

Tejas Mehta has joined RBL Bank as CTO. He was NEXT100 Winner in 2017. Mehta had earlier worked in vari-

ous leadership and managerial positions in esteemed companies like India Infoline, Barclays Bank and Reliance Industries Limited. He completed his MEP from IIM-Ahmedabad, PG Diploma in Management Studies and Bachelors in Electronics.

He is Certified Lead Implementer ISO/IEC 270001:2013 ISO. He also has ITIL Certification from EXIN. ■



Importance Of IoT In Manufacturing Sector

End-to-end IoT Analytics helps in getting a consolidated bird's eye view of all the manufacturing facilities spread across the globe on a single platform with insights into the key performance indicators

By Nabuath Ulla Khan

As we look around the world today, everything is sensor-enabled or controlled. If you walk across a factory floor, you might have dozens of sensors on a single machine that are tracking everything from vibration of multiple axes to pressures to temperatures to mass

flow and much more...you'll also have variable-frequency drives controlling the motor.

But why is the world moving towards having so many sensors around them or the machines, why is that relevant? We've entered the era of the Industrial Internet of Things (IIoT), which is known by a lot of differ-

ent names, like Industry 4.0, Brilliant Factory, 4th Industrial revolution, Smart factory, connected factory and so on...depending on which part of the world you are in.

No matter the name, when you take a deeper look, everyone is talking about the connection between machines, data, and people, which

is mainly driven by adding more and more sensors on the physical machines or products. These sensors on the machines are pulling more data off them, which wasn't collected earlier, that's a lot of information.... This collected data resides everywhere in manufacturing—in Enterprise Resource Planning (ERP) systems, Product Lifecycle Management (PLM) systems, Manufacturing Execution Systems (MES), Supplier Relationship Management (SRM) systems, Customer Relationship Management (CRM) in machine tools and in thousands of spreadsheets, files and folders across the company.

Data also resides outside the enterprise, across the value chain with partners on both supply and sales sides. The goal of sound Industrial Internet strategies is to break down organizational, process, data and system silos and automate the collection of data across end-to-end operations. An enterprise that uses a deeper, wider and smarter analysis of its data will see big operational dividends.

And most of the manufacturing organizations want to take this data, create a single source of truth by

eliminating silos and apply advanced analytics. This helps to push out the most meaningful information to the workforce on ground, on a real time or near to real time basis. In turn, it ensures they are well equipped with the right set of information and insights at the right time with least possible time being spent on large sets of non-productive activities.

Now, let us look at a small portion of the smart factory setup as an example to understand the numerous benefits the organization can capitalize on, by having IoT analytics deployed across the value chain.

The setup shown in the picture talks about how the incoming raw material is converted into a finished product as it moves on the assembly line from one work station to the other using robots or machines. Once the production is completed, the product is packed and dispatched to the end user. Post this, the finished product gets installed at the customer site, the manufacturer or the OEM has ability to track the performance of the finished product in the field.

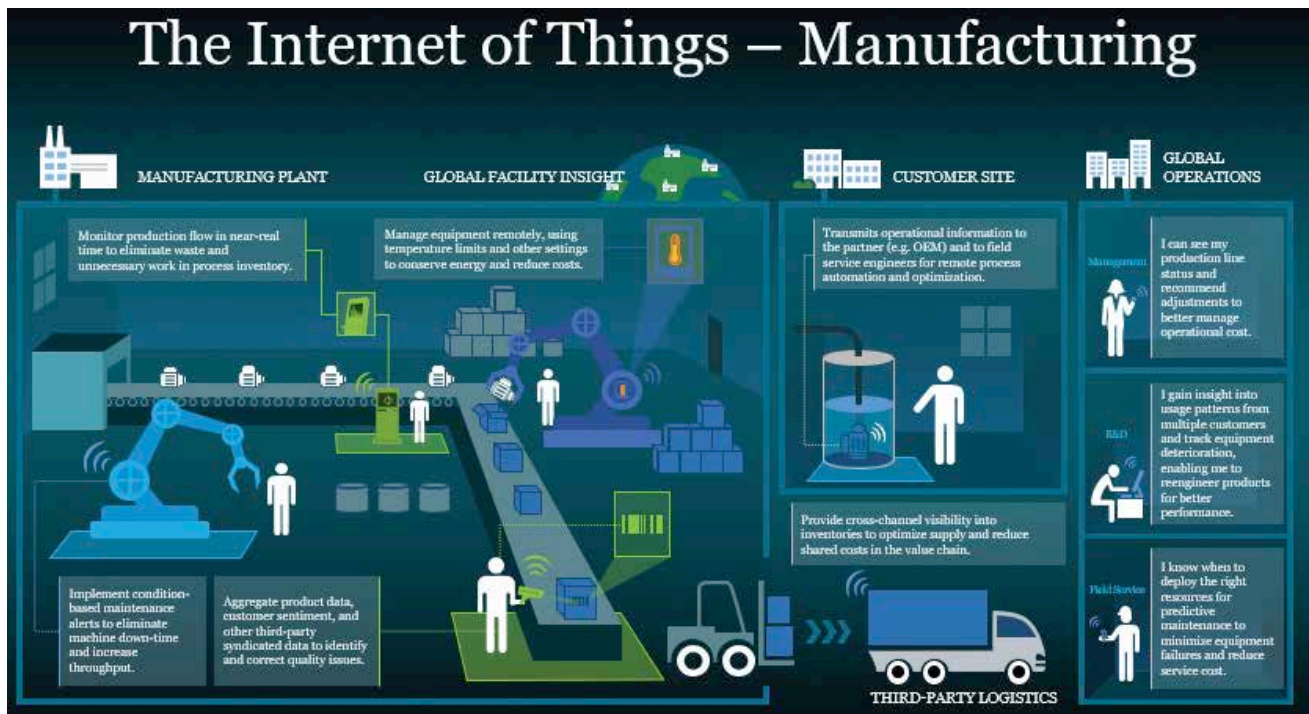
With such a simple setup, we can still say there are multiple touch

points and complexities involved across this value chain. Data gets generated at multiple stages and stored either in silos or on a single source of truth platform, be it on premise or on cloud depending on the organizational IT strategy.

Let's take this example and talk about the various touch points, type of data generated and how the manufacturing organizations can get benefitted at a large-scale using IoT analytics:

Incoming Material – As the raw material enters the manufacturing facility, there is a quality check process in place for all the incoming material, again it can be random sampling or batch sampling or may be 100% testing that happens either manually or automated depending on the organizational maturity and advancements in technology. This step generates a lot of data on the 3 key dimensions of Quality, Quantity and Time by supplier, and then the in-house tested data is validated with the supplier provided quality data.

Manufacturing Plant – Now as the quality approved raw material enters the manufacturing facility, it





Data also resides outside the enterprise, across the value chain with partners on both supply and sales sides. The goal of sound Industrial Internet strategies is to break down organizational, process, data and system silos and automate...

flows through the assembly process on the conveyor belt. Robots do their pre-programmed activity one after the other, until it reaches the end of line or the finished product state. This entire process generates tons of data coming in right from the conveyor belt, Health of Robot, in-spec/out of spec data from one workstation to the other and the end of line quality test.

Customer Site and Third-Party Logistics – Continue to collect data from products once they leave the factory floor (e.g. throughout the distribution process and once implemented into customer sites) as well as, access more data than ever before and integrate with 3rd party syndicated data to improve process and quality control (e.g. use data on regional weather patterns to determine locations where weather conditions will result in higher demand, or view data about fuel and other input prices)

Now that we have a high-level understanding on the various touch points and type of data generated, let us look at a few critical benefits that the organization can achieve leveraging analytics.

Glimpse of few quick wins or top 10 benefits of having end-to-end IIoT Analytics strategy deployed in manufacturing:

1. Manage data remotely from a centralized location and push updates and key notifications to the factory floor, making relevant information available to manufacturing employees.
2. Monitor whether components are arriving at the plant floor as expected, and slow production if needed to reduce or eliminate excess work-in-process inventory
3. Predefine rules for equipment use and plant management (e.g. shut down production or equipment

based on demand or environmental data), to optimize productivity and profitability

4. Establish predictive maintenance schedules – with planned maintenance, cost of operations can be reduced, and throughput can be increased
5. Identify and correct quality issues – with IIoT and the ability to perform Big Data analytics, manufacturers can increase the number of quality checks that are performed, collect more quality inspection data and analyze more data than ever before. This enables them to spot defect patterns and correct them more quickly. This also enables manufacturers to create predictive algorithms so that times/places where quality issues may occur are identified ahead of time.
6. Provide 'single pane of glass' visibility across all distribution/sales channels – this enables better inventory management and savings on logistics and distribution costs in turn reducing redundancies
7. Remote monitoring & diagnostic health alerts of field equipment shared with right stakeholders – An analyst at the customer's OEM or service provider could determine whether the product requires a simple repair, or whether it makes sense to refurbish it.
8. The analyst could identify a spare parts promotion that the customer could take advantage of, so the customer is prepared for future maintenance needs.
9. The information can be used in R&D process to improve the product specifications or design
10. Lastly, end-to-end IIoT Analytics helps in getting a consolidated bird's eye view of all the manufacturing facilities spread across the globe on a single platform with insights into the key performance indicators ■

The author is Practice Head - Manufacturing and IIoT Analytics, SAS India



Healthcare - A Vulnerable Sector For Cybercrimes

According to Radware's 2018-2019 Global Application and Network Security Report, healthcare was the second-most attacked industry after the government sector in 2018

By Nikhil Taneja

The healthcare industry is a prime target of hackers. According to Radware's '2018-2019 Global Application and Network Security Report', healthcare was the second-most attacked industry after the government sector in 2018. In fact, about 39% of healthcare organizations were hit daily or weekly by

hackers and only 6% said they'd never experienced a cyber-attack.

Increased digitization in healthcare is a contributor to the industry's enlarged attack surface. And it's accelerated by a number of factors: The broad adoption of Electronic Health Records Systems (EHRS), integration of IoT technology in medical devices

(software-based medical equipment like MRIs, EKGs, infusion pumps), and a migration to cloud services.

Case in point: 96% of non-federal acute care hospitals have an EHRs. This is up from 8% in 2008.

Accenture estimates that the loss of data and related failures will cost healthcare companies nearly USD 6 trillion in damages in 2020, compared to USD 3 trillion in 2017. Cyber crime can have a devastating financial impact on the healthcare sector in the next four to five years.

The Vulnerabilities

According to the aforementioned Radware report, healthcare organizations saw a significant increase in malware or bot attacks, with socially engineered threats and DDoS steadily growing, as well. While overall ransomware attacks have decreased, hackers continue to hit the healthcare industry the hardest with these attacks. And they will continue to refine ransomware attacks and likely hijack IoT devices to hold tech hostage.

Indeed, the increasing use of medical IoT devices makes healthcare organizations more vulnerable to DDoS attacks; attackers use infected IoT devices in botnets to launch coordinated attacks.

Additionally, crypto mining is on the rise, with 44% of organizations experiencing a crypto mining or ransomware attack. Another 14% experienced both. What's worse is that these health providers don't feel prepared for these attacks. The report found healthcare "is still intimidated by ransomware."

The Office of Civil Rights (OCR) has warned about the dangers of DDoS attacks on healthcare organizations; in one incident, a DDoS attack overloaded a hospital network and computers, disrupting operations and causing hundreds of thousands of dollars in losses and damages.

Why Healthcare?

The healthcare industry is targeted for a variety of reasons. One of the



Indeed, the increasing use of medical IoT devices makes healthcare organizations more vulnerable to DDoS attacks; attackers use infected IoT devices in botnets to launch coordinated attacks. Additionally, crypto mining is on the rise...

reasons is money. By 2026, healthcare spending will consume 20% of the GDP, making the industry an attractive financial target for cyber criminals. And per Radware's report, the value of medical records on the darknet is higher than that of passwords and credit cards.

And as my colleague Daniel Smith previously wrote, "not only are criminals exfiltrating patient data and selling it for a profit, but others have opted to encrypt medical records with ransomware or hold the data hostage until their extortion demand is met. Often hospitals are quick to pay an extortionist because backups are non-existent, or it may take too long to restore services."

One thing is certain: Ransomware and DDoS attacks are extremely dangerous for patients and those dealing

with health issues. Many ailments are increasingly treated with cloud-based monitoring services, IoT-embedded devices and self or automated administration of prescription medicines. Cyber-attacks could establish a foothold in the delivery of health services and put people's lives and well-being at risk.

Recommendations

Securing digital assets can no longer be delegated solely to the IT department. Security planning needs to be infused into new product and service offerings, security, development plans and new business initiatives—not just for enterprises, but also for hospitals and healthcare providers alike. ■

The author is Managing Director - India, SAARC & Middle East, Radware



Regular Patching Your IT Assets - Increases Cyber Immunity

A regular patched system is always less prone to zero-day attacks

By Prakash Kumar Ranjan

Patch management seems to be an endless and thankless bucket of jobs that only get done when there is nothing else to do (thus almost never "on time") or when something is about to break in a big way (or just broken!). It just puts off most of the time, leav-

ing vulnerabilities and functional gaps all over the place. The three biggest challenges for an IT professional are security, reliability and performance. Ideally, an organization's application/software mostly excels at all three but in practice we all know that isn't true. It is a crucial part and parcel for any

corporate IT security strategy or program, but unfortunately for IT managers it becomes equally difficult to do.

NIST (NIST SP 800-45 Version 2) defines patch as "A repair job for a piece of programming; also known as a "fix". A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's website. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches."

Many a times, corporates link the vulnerability management program with Patch Management. But, is Patch Management related with Vulnerability Assessment program?

It is partially but not completely. An organization may have policy of undergoing vulnerability assessment of its IT asset once a year or half-yearly or quarterly, but patch management is an always ongoing program and does not necessarily trigger only after a vulnerability assessment program. However, a vulnerability assessment may project the missing patches in an IT asset so a regular vulnerability assessment may give IT security professional a comfort that the patches has been applied for that IT asset as on day whose vulnerability assessment has been concluded. But as we all know that vulnerability assessment may not be conducted very frequently but patches are released more frequently so patching an IT asset regularly increases the cyber immunity of an organization.

There are various variants of patches:

1. **Hotfix:** A hotfix or Quick Fix Engineering update (QFE update) is a single, cumulative package that includes information (often in the

form of one or more files) that is used to address a problem in a software product (i.e., a software bug). Typically, hotfixes are made to address a specific customer situation.

2. Point Release: A point release is a minor release of a software project, especially one intended to fix bugs or do small cleanups rather than add significant features. Often, there are too many bugs to be fixed in a single major or minor release, creating a need for a point release.

3. Security Patches: A security patch is a change applied to an asset to correct the weakness described by a vulnerability. This corrective action will prevent successful exploitation and remove or mitigate a threat's capability to exploit a specific vulnerability in an asset. Security patches are the primary method of fixing security vulnerabilities in software.

4. Service Packs: A service pack (SP) or a feature pack (FP) comprises a collection of updates, fixes, or enhancements to a software program delivered in the form of a single installable package.

Why IT professionals fail to patch an asset regularly?

a) Some patches may cause performance issues or "break stuff" and thus are often put off rather than dealing with the complications associated with updating.

b) Many organizations do not have proper asset management so if you don't know an asset exists on your network you will never succeed to know the vulnerabilities that exist.

c) A system restart is most often required after patching the asset and getting the downtime for system restart from business is very tough for production systems for an IT team.

d) Many patches are released, so it becomes difficult for an IT professional to determine which patch is applicable for which asset manually unless an automated tool is available to do this activity.

e) Many systems are legacy systems so there is a fear in mind whether the

system would work after the patches is applied and no one wants to own this risk including business.

f) Many small organizations may not have exact replica of production environment in test environment, so they cannot perform testing of patch and even test results may not bring comfort to IT team if test environment is not exact replica of production systems.

g) Often there is a misconception in the mind of IT team that they need to patch only those which is provided by IT security team as missing patch after Vulnerability Assessment of the asset.

Implementing a Good Patch Management Strategy

i. A good patch management strategy ensures that patches are applied in a timely manner and will not negatively affect operations.

ii. Design a patch management policy or program and it should include all assets. A comprehensive inventory of all software and hardware within your environment is a critical piece of any patch management process.

iii. Establish procedures for checking for the existence of available patches, assessing the applicability of the patches and testing the patches.

iv. Critical vulnerabilities that have published exploit code should be given the highest severity weighting and be addressed immediately – not waiting for a patching cycle.

v. Preference to be given to security patches and should be patched on priority.

vi. Do not treat patches with a set it and forget its mentality.

vii. Patch management should leverage system efficiencies but include decision making of skilled and experienced engineers in the patch approval, rollout and upgrade process.

viii. Rollback capabilities to remediate issues. Capabilities and experience to identify the root cause and execute a rollback is super important to keeping a business functional. Patch man-

agement is critical, but not at the cost of uptime to a business.

ix. Some patches may affect production systems, meaning that testing is vital before deployment. Testing should be performed in an isolated test environment, ideally a virtualized mirror of your production environment.

x. Try to leverage the use of automated patching solutions as it addresses major challenge of IT managers that which patch is applicable for which asset and to show the patch status.

xi. If at all, the patching is not possible because of any reasons, the IT team should explore leveraging the virtual patching concept offered by many security solution providers. Virtual patching is the implementation of a security policy meant to prevent an exploit from occurring as a result of a newly discovered vulnerability.

xii. Patch Management strategy should include all types of IT assets, for example endpoints, networks, servers, database, etc. The strategy should also incorporate patching cycle and any deviation/exception of any asset from patching should be documented and approved by the Information Security or IT Strategy committee.

xiii. Deliver messages to end users prompting them, for example, to install a patch or reboot their machine, or informing them about an in-progress deployment.

xiv. Deploy patches on demand at any given point, such as in emergency situations where a vulnerability is suddenly being actively exploited.

xv. Track patch status via its central, dynamic dashboard, and generate reports that can be customized for different types of recipients.

xvi. Define patch management as KPI for IT team and should be measured periodically.

xvii. IT administrators should scan the complete enterprise network for patch update requirements. ■

The author is ICT Security, Risk & Compliance Manager at CNH Industrial



How CIO Can Become The Boardroom Influencer

While CIOs might be gaining some power, their success will depend on how they are developing the right blend of technical, business and influencing skills

By Sohini Bagchi

The phenomenal rise of digital technologies along with changing customer expectations is having a knock-on effect on C-suite dynamics.

While earlier the CEO in alliance with CMO and/or CFO would drive the key business decisions, today, the push for digital transformation has made CIO's role in the boardroom vital. In such a changing scenario, it is

interesting to examine how CIOs can become boardroom influencers and drive organizational change.

CIO's role becoming critical

Various studies have shown and industry experts affirmed that today CIO's are more emboldened to drive organizational changes. For example, a recent research report by Aptio and FT Focus on C-suite leaders and

their changing roles, suggests that the CIO/CTO position now serves a "critical role" in preparing the organization for sustained growth.

"The CIO priorities are shifting as they take a more agile approach to IT strategy," says Sean Kearns, Editorial Director for FT Focus, who believes that CIOs have an enormous opportunity to plot the course of business growth.

However, Kearns tips off that doing so involves achieving alignment with other departments and influence over the boardroom.

Of the organizations undergoing digital transformation in the study, 56% claims to take an 'agile' approach based on constant learning from the business and customers. When it comes to developing products and services, more than two-thirds of global respondents states that digital transformation has strengthened collaboration across the C-suite.

But problems remain...

The expected collaboration between C-suite is also leading to blurred responsibilities, and not all leaders are aligned on business priorities or technology strategy. For example, fewer CFOs and CMOs are aligned with their companies' CIOs in reality, the study shows. The lack of alignment is creating tension between finance and IT, or marketing and IT according to Apptio. About half (47%) of those surveyed even said digital transformation has worsened existing strategic differences between these functions.

For example, the finance head of a leading healthcare firm (who didn't wish to disclose his name) opines that CIOs might be gaining more power within the organization, but many are lacking the communication skills essential to influence their business in order to deliver the change it requires.

There are other pressing concerns in the C-suite. For example, cloud adoption is crucial, but concerns over governance and IT compliance pose challenges for adoption and migration. In such cases, the study also reveals that just 30% of leaders feel confident in IT's ability to govern cloud computing across the business.

At the same time, agile approaches help to accelerate the adoption of new technology, but greater clarity is needed on tracking performance.

Focus on expertise to solve problem

So, while CIOs might be in a position

of power, their success will depend on how they are developing the right blend of technical, business and influencing skills within their organization. The spotlight is therefore on the CIO's expertise in solving these problems at hand.

A study by MIT's Center for Information Systems Research (CISR) brings to light that companies with experienced technologists on their board outperform others in areas such as revenue growth, return on assets and market capitalization growth. In other words, the significant contribution that CIO/CTO's can bring to table gets reflected in the company's financial outcomes.

The analysis shows that out of 1,200 large enterprises with revenues over USD 1 billion, about 24% had board members that were classified as technology experts. These board members included those with experience as a CIO/CTO and expertise in software, digital platforms, big data and innovation, besides substantial years of leadership skills.

According to the study, "Revenue growth over three years for boards with three or more such directors was 17.6% compared with 12.8% for boards without technology experts. Market capital growth over three years was 31.3% compared with 23.3%. Boards with three or more tech experts also had a 34% higher return on assets."

Stephanie Woerner, research scientist at MIT Sloan's CISR states that CIOs and CTOs have a lot to offer to a board. "If a company needs to increase its tech savviness, it could benefit from bringing enterprise technology executives in to advise the board and include them on strategy retreats," she says.

"CTOs and CIOs are going to be people that become really important or attractive to boards," she says, adding that they should have even more interactions with the board than they're having now.

It is also important because doing business in the digital era entails risks ranging from cybersecurity breaches

and privacy issues to business disruptions and missed competitive opportunities. But CIOs with strong digital and business knowledge can offer better and unique learning opportunities to their team and the entire organization.

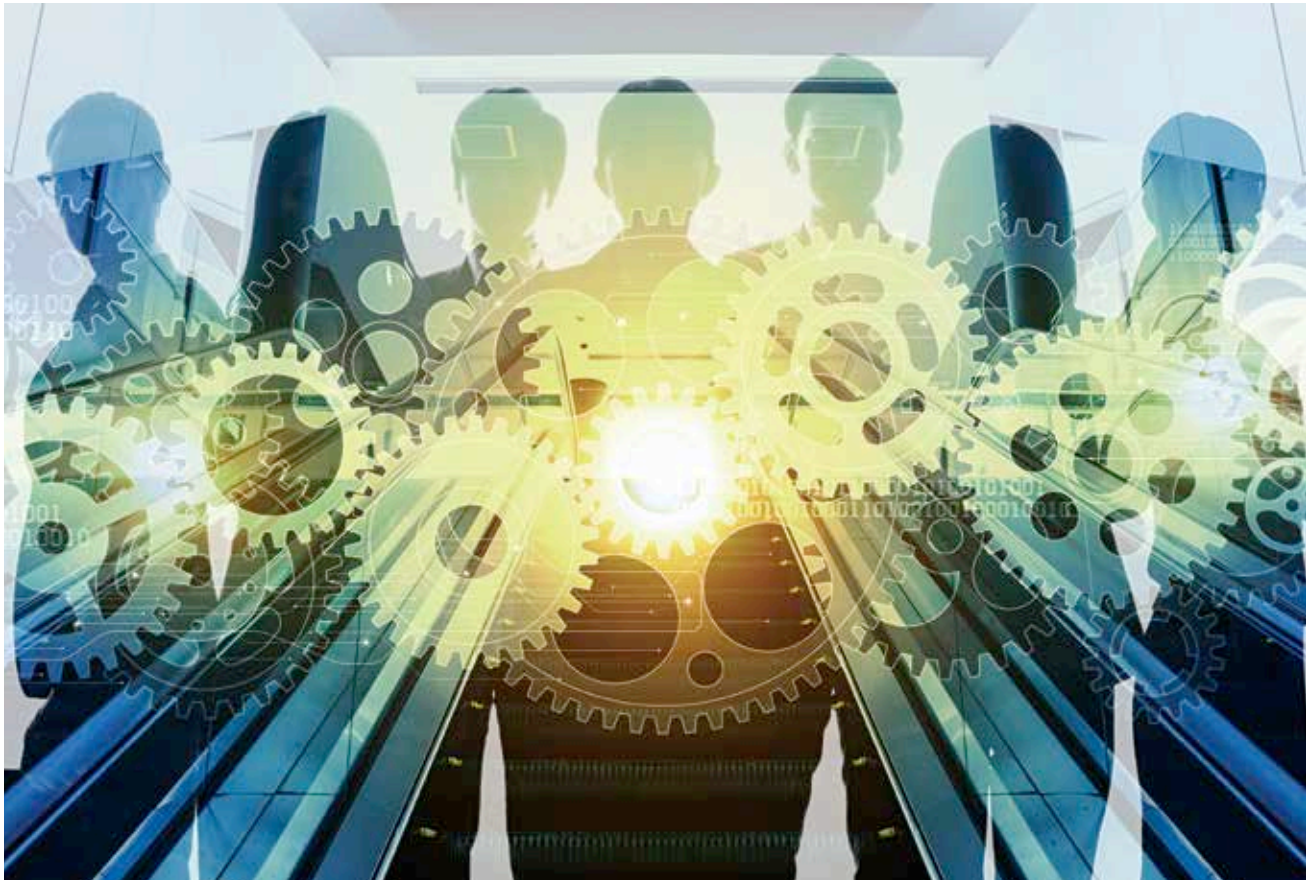
More power to the CIO

Backed by a digital-savvy board, the CIO has the potential to become an influencer to the board, believe experts. As Naveen Gulati, CIO of Ginnar Soft notes, "The CIO can leverage digital technology as an opportunity to drive organizational strategy. For example, s/he should make data and analytics a top company priority and design digital transformation towards business goals."

For example, the CIO can engage digitally-savvy customers, by teaming up with the CMO. Together, they can identify behavior patterns, predict trends as well as analyze profitability of products and services so they can be flexible in offerings. Or involve himself in the recruitment process where HR collaboration with IT can make a big difference to companies.

CIOs must boost collaboration, just like he is involved in boosting efficiency or cutting costs. As the entire organization faces the digital disruption challenge, it's up the CIO to take the lead and explain other decision makers on tech-based improvement and innovation. As Harnath Babu, CIO at KPMG states, "CIO can encourage the C-suite on how employees can have access to adequate training resources in order to support their professional development and equip them for digital transformation."

In every sense, the CIO has the opportunity to move away from their traditional IT-focused role, to become a business leader. As Babu opines, "By honing their leadership skills, being open to collaboration with other department heads and ensuring their IT teams are adequately skilled for digital transformation, CIOs can firmly position themselves as boardroom influencers." ■



What IT Managers Really Want From Their Organization?

A new study reveals that the first thing CIO/CTO wants in the workplace is transparency from their leaders

As technology permeates almost every business area and functions, the board and CEO have high expectations from their IT leaders, including CIO/CTO and senior managers to enhance business value with the effective use of technology. But ever thought what these senior technology managers want from their organization or consider important before they select their employer?

It is not just the fancy tables and the quantifiable perks, as many would think. IT managers are more inclined towards intangible benefits, such as the openness of company leaders, charitable giving initiatives and the company's brand values, according to a new report released by job site Indeed that exclusively polled tech managers, including CIO/CTO/CISO and other senior tech leaders, on what they

value the most at their workplace in terms of culture and ethics.

Almost all CIOs value transparency

When Indeed asked tech leaders their most important to them, or any specific characteristics they value the most in a company, there were a variety of responses, and the most prominent one in their list was transparency from leadership. Nine out of 10 CIO/CTOs consider transparency to be most important, closely followed by what the company is giving back to the community (79%) and how the company shares their values (78%).

Flexible work hours are important

Flexibility is something people often associate with tech. The study found

a common theme that emerged was self-improvement, whether in the form of employee development or tuition reimbursement initiatives (32%) or health and wellness programs (30%). In-office perks, such as free snacks and beverages and other entertainment were surprisingly found to be less important to workers, suggesting their seriousness is more on contributing to their organization.

More flexibility and advancement in a new job

When evaluating a new position, the study found that IT managers consider pay to be most important (this applies to managers of every department). But a number of factors follow. One, they prioritize flexibility in hours and location (92%); the opportunity for career advancement (91%); oppor-

tunities for learning and education (91%); and whether the company has a reputation for ethical behavior (90%). Surprisingly, even though 'pay and benefits' is the top consideration when choosing a new job, 92% said they would be willing to make less money in exchange for one of the other factors listed.

Diversity is important in every area of business

Diversity is crucial to today's IT leaders as it is to an increasing number of workers in every industry. When Indeed asked about the value of diversity in a variety of settings—in leadership, the company, their department, and on their team, over eight in 10 say each one is "somewhat" or "very important" to them. Organizations should make sure



that 83% technology leaders value a flexible workplace. Specifically, techies site variable work hours (59%) was most important, followed by the ability to work from home (25%), and remote-work options (14%).

The study concludes that offering flexibility at work makes it easier for workers to manage different areas of life, such as caring for children and aging parents, as well as taking care of other chore. And since flexibility tends to lead to productivity, it's a win for employers, too.

Top perks and benefits involving self-improvement

When Indeed asked CIOs and other tech managers which benefit they value most at their current company,

The study concludes that offering flexibility at work makes it easier for workers to manage different areas of life, such as caring for children and aging parents, as well as taking care of other chore

efforts and initiatives are in place to promote diversity and inclusion—both among candidates and existing employees. And be sure to publicize these efforts throughout your recruiting process, on the company website, and through social media.

The study concludes therefore that apart from pay and benefits, CIO/CTO and other IT managers do care for workplace flexibility, career advancement and continuous learning, organization's ethical and brand reputation and a diverse and inclusive workforce when it comes to selecting their employer. Organizations understanding these parameters will help the tech leader to make a difference in his career as well as in attaining their overall organizational goals. ■



CIOs In Banking And Financial Firms Still Grappling With Cybersecurity

While the financial services industry is relatively mature in terms of its software security posture, organizations are increasingly facing cyber attacks

When it comes to cybersecurity awareness and practices, CIOs in the banking and financial services industry are at a much higher maturity curve than their peers. Despite their awareness and concerns about online threats, a new study found that bank-

ing organizations are struggling to manage cybersecurity risks, with many CIOs acknowledging that they are still not doing enough to protect their systems, networks and data.

The Synopsis report, based on a survey of CIOs and IT security practitioners from global financial services organizations conducted by Ponemon

Institute, found that more than half of these firms have experienced theft of sensitive customer data or system failure and downtime because of insecure software or technology.

Besides, the study shows, banking and financial firms' CIOs are struggling to manage cybersecurity risk in their supply chain and are failing to assess

their software for security vulnerabilities before release.

“While the financial services industry is relatively mature in terms of its software security posture, organizations are grappling with a rapidly evolving technology landscape and facing increasingly sophisticated adversaries,” says Drew Kilbourne, Managing Director of Security Consulting for the Synopsys Software Integrity Group.

There are three key findings from the study:

- 1. Most FSIs are ineffective at preventing cyberattacks.** As per the study, more than half of respondents have experienced system failure or downtime (56%) or theft of sensitive customer data (51%) due to insecure software or technology. Predictably, the study shows that more organizations are effective in detecting (56%) and containing (53%) cyberattacks than in preventing attacks (31%).
- 2. CIOs are struggling to manage cybersecurity risk in their supply chain.** Nearly three-quarters (74%) of CIOs in the FSI segment were concerned or very concerned about the security posture of third-party software and systems. Despite this concern, only 43% of respondents said their organiza-

tions impose cybersecurity requirements on third parties involved in developing financial software and systems. Furthermore, only 43% of respondents said they have a formal process for inventorying and managing the open source code in their software portfolios.

3. FSI organizations are failing to assess their software for security vulnerabilities before release.

While most organizations follow a secure software development life cycle (SDLC) process, respondents reported that their organizations test, on average, only 34% of all financial software and technology developed or in use by their organization for cybersecurity vulnerabilities. For the software and technology that is tested for vulnerabilities, only 48% of respondents reported that security testing occurs in the pre-release phases of the SDLC, such as the requirements and design phase or the development and testing phase.

How banking CIOs can keep hackers at bay

While it is impossible to make an organization bulletproof, the survey results show that organizations are aware that they have a problem. Hence, here are some key takeaways for CIOs

in financial organizations to keep the hackers away – securing their turf both from an external as well as internal perspective:

- Using automated tools that can help developers find and fix bugs before pen testers find them later, when they take more time and money to fix.
- A second fundamental is to address third-party risks, because if they can get hacked, you can get hacked. So organizations should require their vendors to test their software during development, to demonstrate compliance with industry security standards and to use an independent measurement of their SSI.
- CIO/CISOs should secure the supply chain from insider threats. This often requires new workflows and governance processes.
- Organizations should make the workforce security savvy by proper security training and empowerment. This initiative should be led by CIO/CISO/CTO or a security expert in top management
- Make sure devices and servers are configured correctly. For this, the IT or security team should be on the lookout for patches and install them immediately.
- An end-to-end encryption helps. CIOs should ensure they have secure encryption key management.

“There is no single right approach to software security but this study clearly shows that there is a significant need for improvement in supply chain risk management. There is also an opportunity for many organizations to expand the scope of their software security programs to cover all their business-critical applications and shift their efforts further left in the software development life cycle,” says Kilbourne.

Much of that is the digital equivalent of locking the safe and the doors at night and turning on the security system. The study researchers believe, any organization that does all that will be better than above average. ■





Organizations And Customers Opting For Passwordless Future: Study

They are going for biometric authentication, Bring Your Own Identity (BYOI), Multi-factor and Risk-based Authentication methods

More and more organizations and customers are opting for passwordless future and instead going for biometric authentication, Bring Your Own Identity (BYOI), Multi-factor and Risk-based Authentication methods, according to LoginRadius, a leading

cloud-based customer identity and access management platform.

Issue I - The Easy vs Secure Conundrum

Customers want fast, easy access to every site or app they use. Yet, 90% of internet users have data privacy concerns. If customers aren't given

secure, yet easy login and sign-up access, they'll take matters into their own hands. They'll create vulnerable passwords that jeopardize your digital infrastructure and their private data.

Why Passwords Fail

- Password complexity is weak: Passwords may meet complexity, yet

still be considered weak because of password dictionaries.

- Passwords aren't unique: People reuse passwords and newly leaked dictionaries contain previously leaked passwords.
- Password follow patterns: In most cases, the top 100 patterns will crack the majority of passwords in an organization.
- Password cracking is easy: With available hardware resources, it can take seconds to brute force most passwords.

Top 3 Password Hall of Shamers

81% of hacking-related breaches leveraged stolen and/or weak passwords? Bad passwords are so prevalent.

- 59% reuse their passwords everywhere – at home and at work.
- 87% of millennials reuse passwords, despite knowing better.
- Over 70% of employees reuse passwords at work for all their work apps.

Issue II- Interrupted Customer Journey

- One-third of online shopping is abandoned due to forgotten passwords. It is also a threat to the health of your business.
- A recent study shows that 18.75% of cart abandonment occurs during password resets.

This indicates that even when consumers are committed to buying something online, delays make people reconsider purchasing. For this reason, smart enterprises will want to eliminate any obstacles in the conversion process.

Here are some ways they do this.

Customer Access Solutions

- **Passwordless:** An authentication method is called passwordless when no password is being stored. Instead, your customers gain access to your website or app through an access code or link that you send to their phone or email. One of the most popular passwordless methods used today is One Time Password (OTP). A no-password

solution means better security and no-hassle sign-ins.

- **Biometric Authentication:** Within the past few years, biometric authentication has become quite common and includes:

- **Fingerprint:** Using TouchID, users authenticate in real-time by scanning their thumbprint on a mobile device that is matched to an image on file.
- **Facial Recognition:** FaceID allows a user to authenticate in real-time by taking a selfie that is then compared to an image on file.
- **Voice Authentication:** This technology analyzes a customer's voice for unique characteristics, and then matches that to a voiceprint on file.
- **Gesture Biometrics:** Another futuristic passwordless method being used today is called gesture biometrics. According to BioCatch, the software company who provides the Royal Bank of Scotland with this functionality, this system can detect imposters with 99% accuracy.

Customer and Business Pain Points

Issue 1 - Too Many Passwords

Password fatigue happens due to several online interactions like:

- Bill viewing or payment for telephone/cable/utilities
- Reviewing or paying for health/medical services
- Inquiring about government services
- Using software/apps for work
- Engaging with social media
- Making online purchases
- Managing your banking/Finances
- Signing up or into educational portals
- Contributing to chat forums, review sites, etc.

Issue 2 - Weakened Passwords

A dangerous side-effect of password forgetfulness is the use of easily guessable (AKA hackable) passwords. A weak password not only puts consumer data at risk—it puts the companies that hold this data at risk, too.

Some extra authentication methods may include a notification email sent to the user or administrator. Here are some ways they do this.

- **Bring Your Own Identity (BYOI):** CIAM software allows you to connect your app or website to a 3rd party provider that your customer uses. This way, your customers can sign in to your app or website using their existing credentials instead of creating a new password. Ex: Sign In with Apple. Therefore, anyone who uses Apple will never have to remember a password when connecting to integrated 3rd-party apps. In addition, users can hide their emails, allowing for greater privacy and security. A common example of BYOI is social login, where a customer may use Facebook or other social platforms to access a website or app.
- **Multi-factor & Risk-based Authentication:** Instead of asking people what they know (passwords), many enterprises are using authentication methods based on what people have—their smartphones. The common term for this is SMS-based authentication. With these criteria, you can create a Risk Profile that recognizes out-of-character customer actions.

Judging by the numbers alone, chances are that many of your customers may be putting your business at risk due to bad password practices. That's perhaps the strongest reason why passwordless authentication is preferred by consumers and enterprises alike. A customer identity and access management solution can provide passwordless, yet secure authentication options for your customers.

While passwords might not be entirely ghosted yet, the majority of consumers agree: They need secure, simple, and seamless sign-ins across all devices. For businesses who fail to use passwordless technology, this can be a death sentence. That's why smart enterprises aren't waiting for a passwordless future—they're preparing for it now. ■



Effective Security Performance Management Need Of The Hour

Nearly two in five (38%) of enterprises admit that they have lost business due to either a real or perceived lack of security performance within their organization, according to a BitSight study

Nearly two in five (38%) of enterprises admit that they have lost business due to either a real or perceived lack of security performance within their organization, according to a BitSight study.

Based on a survey of 207 security decision makers with responsibility for risk, compliance, and/or communications with boards of directors, the study explores the organizational misalignment and technological complexities that commonly prevent organi-

zations from realizing effective security performance management (SPM).

Some of the findings of the study include:

Effective security performance management drives business wins and better security outcomes.

Nearly three-quarters of C-level respondents say that improved security performance measurement would greatly or significantly improve company financial performance, while the majority of respondents overall agree that improved measurement would improve company business continuity (82%) and company reputation (81%).

Additionally, companies that have formal security performance metrics are more likely to successfully manage security: They are nearly two times more likely to develop security policies, update security technology and perform security trainings.

Their investment decisions and strategies are also better trusted by executives and board members: using formal security metrics means security leaders are likely to see a 10% or greater year-over-year increase in security budget.

Commercial success is at risk due to missteps in effectively measuring security performance and communicating it to external stakeholders. 79% of security decision makers surveyed say customer and partner demands for cybersecurity reporting have intensified, but decision makers also say customers are partners receive some of the least accurate reporting of any security stakeholder.

Additionally, 82% agree that customer and partner perception of security is increasingly important to the way their firm makes decisions.

Metrics are critical to understanding and improving communication around security performance, but there is vast room for improvement in current methods. 63% of respondents have introduced formal security performance metrics, but four of the five top



Commercial success is at risk due to missteps in effectively measuring security performance and communicating it to external stakeholders. 79% of security decision makers surveyed say customer and partner demands for cybersecurity reporting have intensified...

reported measurements lack context and paint an incomplete picture of security performance and can leave companies blind to potential risk.

These metrics include: The number of malware incidents blocked (used by 50% of respondents); the number of intrusions blocked by a firewall/network security (50%); the percentage of filtered phishing/malicious emails (45%); and the number of data loss prevention incidents (40%).

Cybersecurity risk ratings emerge as an early security metric bright spot. 45% of respondents report using cybersecurity ratings,

making it the third-most common metric overall. 49% of respondents say that security ratings are their top preferred metric. Derived from objective, verifiable information, security ratings provide a strategic and contextualised measurement of security performance.

43% of companies using cybersecurity ratings report them out to customers and partners, and 63% report them up to the board, indicating that security ratings are emerging as a top method for security performance communication across key company stakeholders. ■



Majority Of Working Millennials Hooked On Checking Emails In India: Study

More than 61% working professionals between the age of 25-32 choose to open their emails every time a new email notification appears

Email is the most commonly used tool for communication and collaboration at work. Consequently, most inboxes are noisy and way too crowded. Almost 50% of the employees surveyed said they spend at least an hour a day checking emails, including 16.2% employees that spend more than 4 hours on their inboxes, according to a new research conducted by Hiver, a SaaS based email collaboration tool that improves visibility and information exchange across organizations using shared inboxes.



This survey exhibits a worrying number of employees exercising emails and how a colossal amount of time is spent by them on checking emails. More than 61% working professionals between the age of 25-32 choose to open their emails every time a new email notification appears, whereas 33% of the employees tend to check their emails every few hours.

Hiver conducted a survey in order to gauge how effectively employees working across different organizations consume emails. Among those surveyed, about 80% are working in startups and 20% are working in corporates. The survey was conducted among 450 respondents in India.

Interestingly, while 60% of the employees surveyed agree with the need to clean their inbox time and again, almost 40% of the employees don't wish to clean their inboxes at all. Employees choose different techniques and procedures to clear their mailboxes. 32% of employees used email based filters, and about 37% employees wish to move the important events to the calendar. About 35% convert tasks into a to-do list, making it possible for the employees

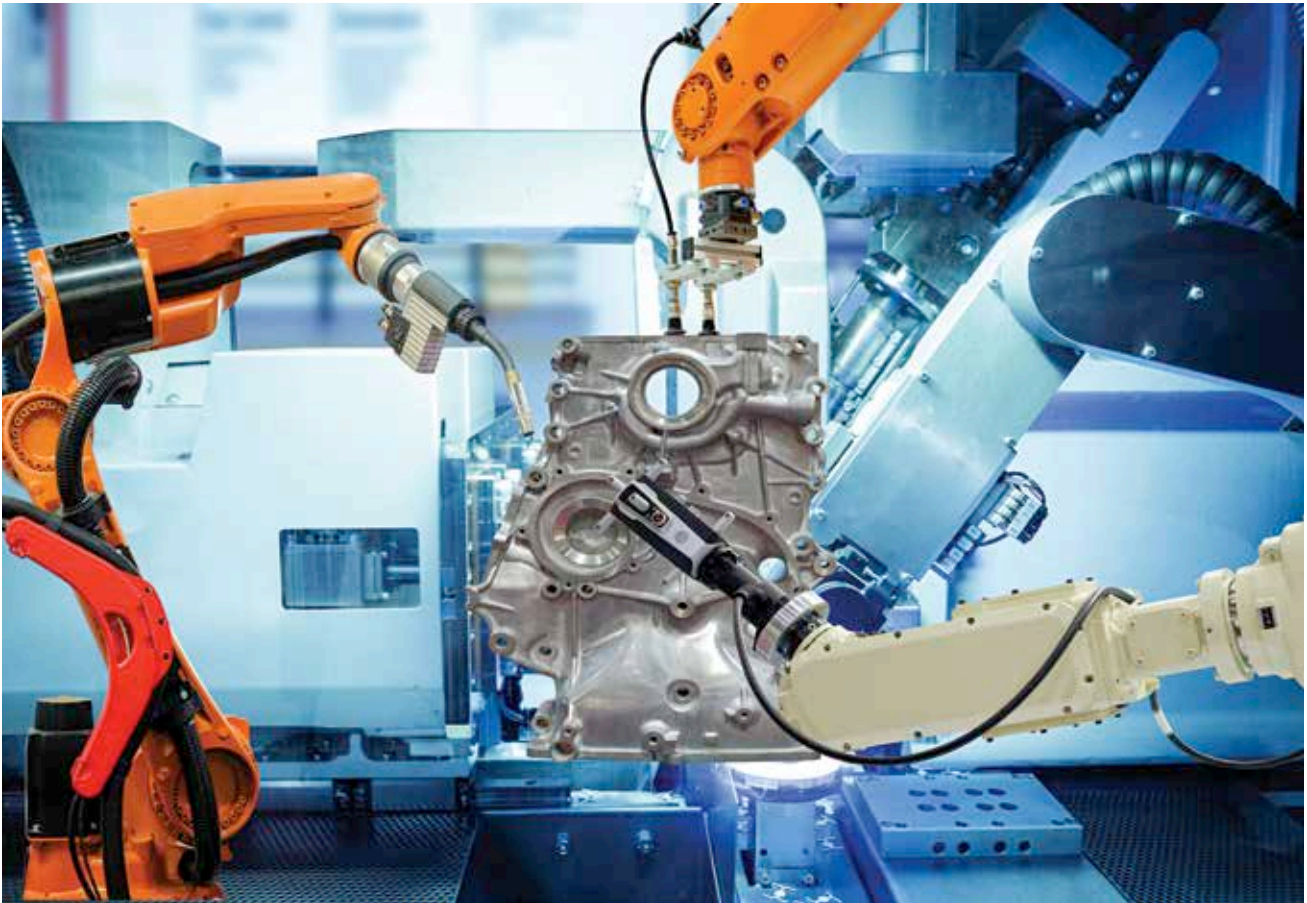
Interestingly, while 60% of the employees surveyed agree with the need to clean their inbox time and again, almost 40% of the employees don't wish to clean their inboxes at all

to use their mailbox effectively. The report also indicates that 76% of respondents say that they read more than 40% of the mails they receive and 55% of the respondents act on every email as soon as it comes in. Given that almost a third (32.4%) of the respondents receive more than 50 emails a day, ample time is spent by them on only checking their emails.

To add to that, half of the respondents say that the maximum number of emails received are from their own organization, either from the members of their own team or others working within the organization. This raises the question - Is internal email communication cluttering up employee inboxes? And how is this affecting employee productivity? This finding is particularly interest-

ing, given that employees can often feel quite productive just by having cleaned out their email inbox, despite perhaps not creating any value for the organization.

Niraj Ranjan Rout, Founder of Hiver, said, "Professionals across organizations rely heavily on email for communication and exchange of information. Our survey highlights how email impacts worklife for many, and while it can be a tremendously useful tool, it can also deter productivity. Our inboxes are packed with valuable information, and in order to organise our work better, we must manage, classify and prioritize emails in an efficient manner. If not, the email overload can tend to become a roadblock in reaching the desired results. It's about how to work smarter, not just harder." ■



Bots Tough To Deploy For Most Organizations: Study

On average, only 39% of bots are deployed on schedule, and it typically takes 18 months on average to successfully push bots live into production

Robotic Process Automation (RPA) and Robotic Desktop Automation (RDA) is highly effective in streamlining work – though achieving and maintaining those results isn't as simple as it seems, according to Pegasystems' survey.

RPA has become a buzzworthy solution for organizations under pressure to modernize their legacy IT infrastructure and stay competi-

tive. Gartner recently reported that "RPA software revenue grew 63.1% in 2018 to USD 846 million, making it the fastest-growing segment of the global enterprise software market." It's often positioned as a quick and easy path to digital transformation by automating cumbersome and mundane processes. To find out if robotic automation lives up to the hype, Pega polled more than 500 decision makers from

global businesses in a mix of industries currently using RPA and/or RDA.

The survey found most respondents gain significant value from automating their operations with bots. In fact, 67% said that robotic automation is even more effective than they originally anticipated, while only 8% felt it was less effective than expected.

But getting to that point and staying there can be more challenging than expected. Survey respondents report the following issues:

- **Bot deployment isn't as easy as it sounds:** Organizations are spending more time and effort getting bots up and running than anticipated. Deployment ranked as respondents' top bot challenge,



The survey found most respondents gain significant value from automating their operations with bots. In fact, 67% said that robotic automation is even more effective than they originally anticipated, while only 8% felt it was less effective than expected. But getting to that point and staying there can be more challenging...

and half (50%) said bots are harder to deploy than they first thought. On average, only 39% of bots are deployed on schedule, and it typically takes 18 months on average to successfully push bots live into production.

- **Bot lifespans aren't all that long:** Inevitable changes to the underlying enterprise architecture will likely lead to increased bot breakage over time. Already, 87% of respondents experience some level of bot failures. 44% said the amount of bot breakage is small, but 37% said it's a moderate amount, and 6% think it's quite large. Overall, maintenance ranked as the second biggest problem bot users face. On average, organizations think bots

will last approximately three years, though their bot initiatives are only 1.8 years old.

- **Bots need more maintenance than expected:** With bot breakage a near certainty, RPA and RDA can't be viewed as a set-it-and-forget-it task. 41% of respondents said that ongoing bot management is taking more time and resources than expected. Bots also add another layer of complexity to IT. How much? 38% felt their use brought more complexity than expected, while 26% said they added more 'shadow IT' issues than expected. Despite these issues, one thing is clear: Bots deliver on their promise when deployed in the right situations. 66% think bots bring more value and

ROI than originally expected, while only 13% have been let down by the amount of value and ROI they've seen. In addition, respondents ranked the top benefits of robotic automation as:

1. **Better work production:** Respondents said 'enabling people to work more efficiently, effectively, and accurately' ranked as the biggest benefit of bots (picked by 51% of respondents).
2. **Healthier bottom line:** 'Reducing overall business costs' ranked second with 45%.
3. **Happier employees and customers:** 42% report the top benefit is improved employee experience, just edging out 'improving customer experience' (40%) for third place. ■



Google Cloud

PRESENTS



SMART STRATEGIES
WINNING TEAMS • 2019

BRAND OF
CIO&LEADER ITNEXT

Technology Premier League 2019

Smart Strategies Winning Teams

Delhi

📅 20th – 21st Sept 2019

📍 Pullman & Novotel, Aerocity

Mumbai

📅 4th – 5th Oct – 2019

📍 Grand Hyatt, Santacruz

Bangalore

📅 11th – 12th Oct 2019

📍 Sheraton Grand, Whitefield



To know more, visit tpl2019.com



What They Said @TPL



Delighted to be a part of the TPL. It's an amazing format, the case studies are for real and you really have to work hard to solve it to showcase it to the jury. I really appreciate the efforts by 9.9 Group."

Jitendra Singh
CIO, JK Cements



The whole experience and the journey we had over 2 days during the TPL was quite enriching, exciting and rewarding. There was good competition between the participating organizations and valuable inputs from Google Cloud as well. Also, this was a great team building exercise for us as everyone worked together the whole night on the solution and presentation."

Anup Bhasin
VP – Technology
EXL Service



Feels like we are back to college; all of us are working and brainstorming on the project. Its really challenging and we have truly enjoyed it."

Jai Prakash Sharma
EVP - Technology
Operations,
InfoEdge India



I think this is one of the best & most exciting events which I have faced – The Technology Premier League —where we have the best enterprise technology teams competing with each other to win the title. Thanks to 9.9 Group & Google Cloud for organizing this event."

Rajiv Nandwani
Director & VP - Global
Information Security,
Innodata



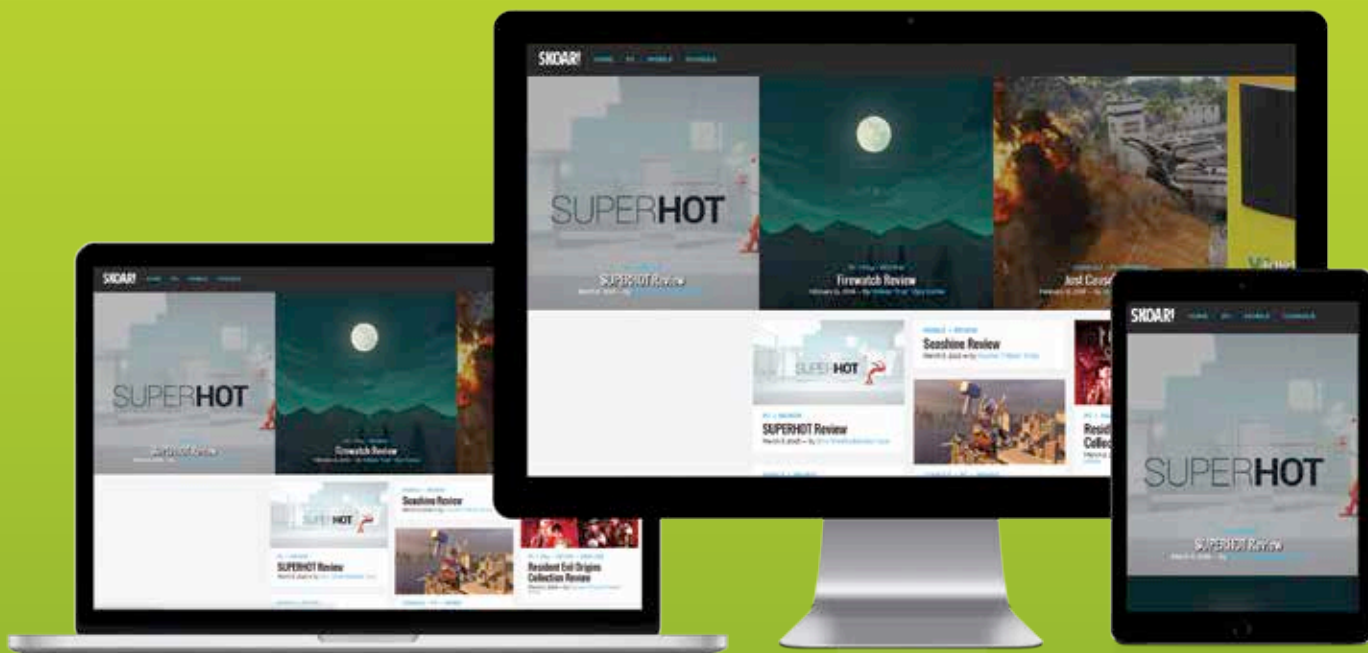
It's a wonderful opportunity for the IT team who is always in the backdrop to show their technology and business skills and get recognized."

Sachin Jain
CIO,
Evalueserve

For more information, please contact:

Vivek Pandey

vivek.pandey@9dot9.in, +91 98714 98703



skoar.in



facebook.com/SKOAR



@skoar

**Like us on Facebook
and follow us on Twitter**
to get the latest game news, reviews and more.



Two times
the revelation



Anish Sharma

Head - IT, elnfochips

A TECH BOOK I LOVE READING

ISACA CISM Review Manual

MY FAVORITE SUPERHERO

Spiderman



MY FAVORITE CUISINE

Rava Masala Dosa



A PLACE I WOULD LIKE TO VISIT REGULARLY

Cherai Beach in Kerala



AN ENTERPRISE TECH THAT'LL HAVE MAJOR IMPACT BY 2020

RPA

MY PEER IN THE IT COMMUNITY

Jignesh Parekh,
Head - IT, Ratnamani
Metals & Tubes



Jignesh Parekh

Head - IT, Ratnamani Metals & Tubes

A TECH EVENT I ATTENDED RECENTLY

Digital Transformation Event organized by the Gujarat Computer Association in conjunction with NASSCOM and the Government of Gujarat in Vadodara, August 2019

MY FAVORITE SPORTSPERSON

Virat Kohli



MY FAVORITE AUTHOR

Chetan Bhagat



A TECH IDOL WHOM I FOLLOW

Steve Jobs



MY FAVORITE COLOR

Blue

To follow the latest in tech,
follow us on...



facebook.com/digitgeek



digit.in/facebook

डिजिट अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध है। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओं से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यू से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओं में उपलब्ध होगा।

di9it.in
NOW IN HINDI



www.digit.in/hi
www.facebook.com/digithindi

डिजिट

DATA CENTERS DESERVE

PERFORMANCE. RELIABILITY. CONSISTENCY.



EXPERIENCE

For more than 30 years, Kingston has been an integral component in the IT backbone of Fortune 500 companies. An experienced business solutions partner, Kingston offers products with consistent and reliable performance along with award-winning solutions required by enterprise environments.

SATA 3.0 (6Gb/s)



Server Virtualization



Cloud Computing



IT Applications

MEMORY | SSD | USB DRIVES | FLASH CARDS

For sales enquiry: sales_india@kingston.com
Service toll no.: 1860 233 4515
RMA/WARRANTY: services_india@kingston.com,
For technical support: techsupport_india@kingston.com



Quality of Service (QoS) | Predictable Low Latency | Consistent I/O Delivery

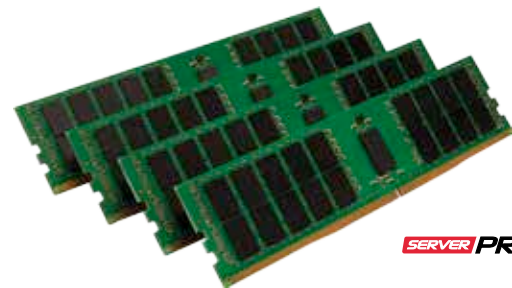
Enterprise Solid-State Drives (SSD)

Incredible Speeds With Full Security Suite.



Server Memory

Accelerate Performance



SERVER PREMIER



©2019 Kingston Technology Far East Co. Ltd (Asia Headquarters) No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan, R.O.C.
All rights reserved. All trademarks and registered trademarks are the property of their respective owners. MKF - 862.1