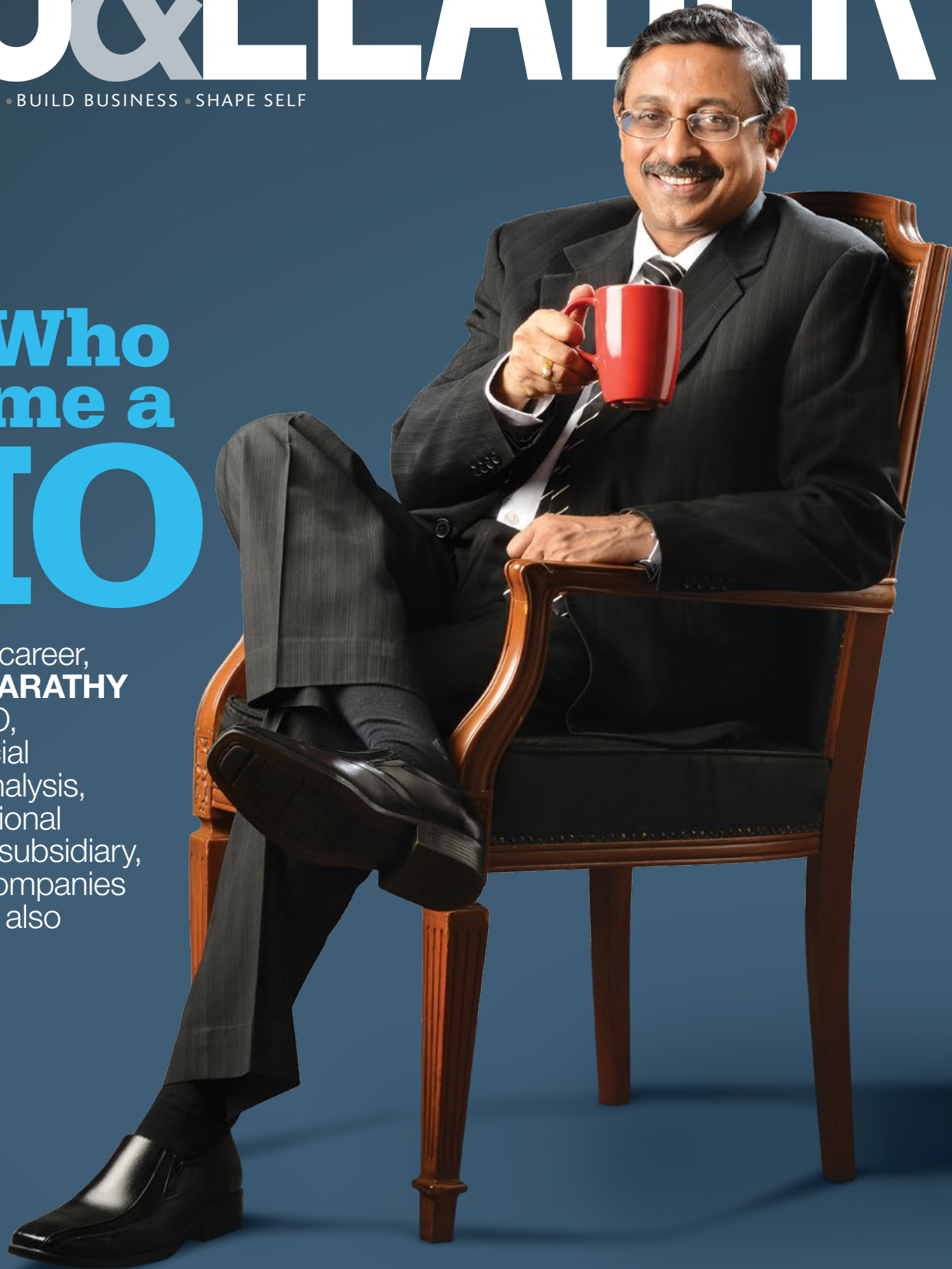# CIO&LEADER

TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

CFO Who Became a CIO

In his illustrious career,
V S PARTHASARATHY
has been a CFO,
controller-financial
planning and analysis,
headed international
operations of a subsidiary,
and acquired companies
abroad. He has also
managed IT.

Page 16

INTRODUCING A SYSTEM

1,000+

IBM PureData System for Operational Analytics is designed to handle 1,000+ concurrent operational queries.[3]

Now more than ever, data and analytics are transforming the way companies do business. This transformation brings with it tremendous opportunity and creates quite a few headaches for the IT department.

The problem is in the nature of big data itself. It's growing in volume and constantly changing, and the rigid, custom data services that companies traditionally built just can't keep up.
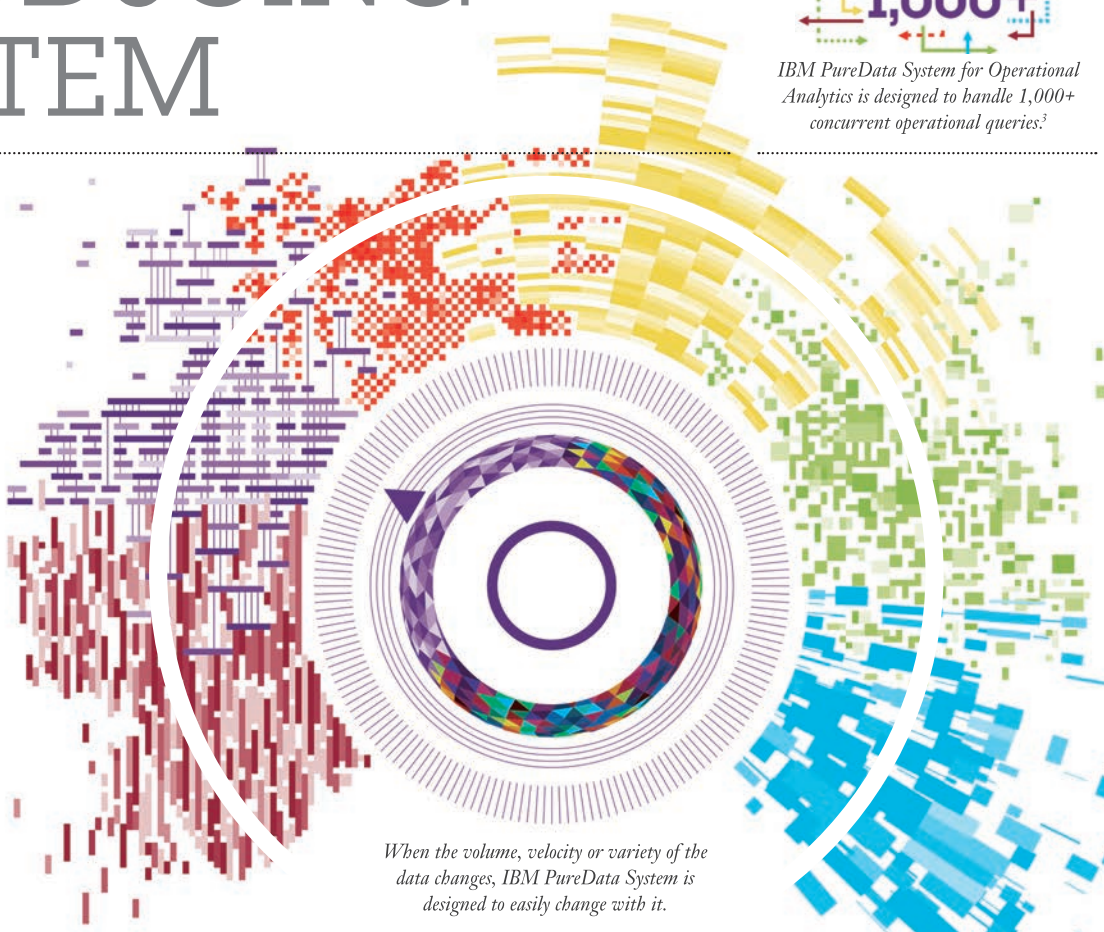
When the volume, velocity or variety of the data changes, IBM PureData System is designed to easily change with it.

100+

With IBM PureData System for Transactions, you can consolidate more than 100 databases onto one system.[1]

AN EXPERT SYSTEM

Introducing IBM PureData™ System, a new addition to the IBM PureSystems™ portfolio designed specifically around data. Like all PureSystems offerings, the PureData System comes with the expertise of thousands of deployments built in. These patterns of expertise mean that no matter what you

THAT ADAPTS TO THE DATA.

want to do with your data— transaction processing, operational analytics or deep analytics—virtually every aspect of the experience will be simplified with an integrated management console and comprehensive system support.

What's more, PureData System's hardware and software are integrated by

design for today's high-performance data workloads. Its deep analytics model, for example, runs analytics queries up to 100 times faster than traditional custom data warehouse systems.[2]

DATA MANAGEMENT AND ANALYSIS MADE SIMPLE

As our markets and economy become increasingly oriented around data in all its varieties, IBM PureData System is designed to easily and simply

respond to all of it. See how simple it can be at **ibm.com/PureDataSystem/in**

LET'S BUILD A SMARTER PLANET.

IBM®

EDITORIAL

YASHVENDRA SINGH | yashvendra.singh@9dot9.in

CIO 2.0 Today's CIO has to assess a complex tech issue along with its crucial financial implications

Those who think leadership is just about managing people need to rethink. To become an influencer and someone who empowers others, you need to untiringly move ahead on the personal and professional growth path.

One of the ways through which an enterprise technology leader can progress on this road is by broadening his horizons. We completely agree that a CIO is almost always busy in the trenches but it is worthwhile for him to take time off his routine and get to know his corporate and employees better.

Visionary CIOs have already realised that their real business partners are those outside of their IT departments. Such CIOs are aware of the potential of new technology.

An enterprise technology leader cannot keep waiting for someone to hand over a winning strategy to him.

By getting to know the business, customer, competition and industry trends, a CIO can get valuable insights. Such insights are the building blocks of a great strategy. A great leader can weave all the insights gathered into an actionable and successful IT strategy.

In fact, as we move ahead, the CIO would have to play a dual role. One the one hand, he would have to ensure the operational readiness of his organisation (data centers are running, security is top-notch, and queries are attended within seconds). On the other hand, he would have to don the mantle of a transformer, who comes up with ideas that unlock strategic opportunities for the company. A CIO would have to assess a complex technology issue along with its crucial financial implications. His success or failure would depend on how well he marries these two radically different profiles.

Then there are those select few CIOs who have undergone a mindset change. While they have a strong grip on technology and are technologists at the core, they don't allow themselves to be looked upon as just fixers of technology. They have shrugged off the image of someone who handles just IT. These CIOs neither shy away from discussing business nor think twice of shouldering new and challenging responsibilities. Our cover story in this issue focuses on one such enterprise technology leader. Throughout his long and illustrious career, V S Parthasarathy, Group CIO of Mahindra & Mahindra, has taken one challenge after another, and overcome each of them successfully. Parthasarathy' leadership journey to the top is certainly worth a read.

In today's world results are accorded greatest importance. However, we believe how one gets there is also vital for lasting success.

Yashvendra Singh

||||||||||||||||||||||||||||||||||||||||||||||||||||||

EDITORS PICK

18

COVER STORY

18 | CFO Who Became a CIO V S Parthasarathy has donned several roles in his leadership journey, proving successful in each one of them

COVER DESIGN BY: **SAMEER KISHORE**
PHOTO BY: **JITEN GANDHI**

CIO&LEADER

46

NO HOLDS BARRED

46 | SHIFTING FROM IPV4 TO IPV6

Mahesh Gupta, Geo-Lead, BN Sales, Cisco India & SAARC, talks about different challenges in migrating from IPV4 to IPV6

48 | TECH FOR GOVERNANCE: WHAT IS ENOUGH SECURITY?

Enough security is not the same thing as absolute security

10 | BEST OF BREED: TECHNOLOGY AUTONOMY BOOSTS PROFITS Profits would increase if employees could choose their own device and applications

37 | NEXT HORIZONS: HACKING BACK IS A BAD IDEA The idea of "hack-back" is best left to 007 and his army of hacker-geeks

Do you have future CIOs in your team?
FIND OUT NOW!

INDIA's FUTURE CIOs

NEXT100
2013

About NEXT100

NEXT100 is the Indian IT industry's premier awards program that identifies and honors 100 experienced IT managers who have the skills and talent to become CIOs and leaders. All NEXT100 award winners are selected through a rigorous and comprehensive evaluation process that reviews techno-commercial, management and leadership skills. The final selection of the award recipients is made by a prestigious committee comprising India's top business and technology leaders

NEXT100 Award Process

- Applicants need to complete the online registration and application form (Last date is 04-Aug-2013)
- All applicants have to take the online psychometric tests that assesses personality traits and leadership style
- Qualified applicants are shortlisted for interview by jury panel. Each candidate is independently interviewed by two jury members
- Reference checks of qualified candidates are done with work supervisors and designated referees
- The list of NEXT100 award winners is announced by the jury, and award winners are invited to attend an all-expense paid gala awards night

How to Refer

You can nominate candidates by going to http://goo.gl/X7kWo. The last date for nominations is 31st July, 2013.

PARTNERS

Platinum Partner

vodafone

Technology Partner

HCL

NEXT100 Book Partner

arkadin
COLLABORATION SERVICES

VISIT WWW.NEXT100.IN TO KNOW MORE

Initiative by

99MEDIA

Event by

IT NEXT

APPLY TODAY AT WWW.NEXT100.IN

Download the NEXT100 App to register and track your application

Google play
Available on the iPhone App Store
Windows Store

ENTERPRISE ROUND-UP
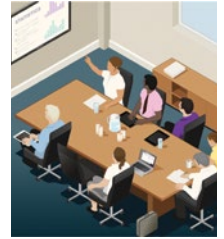
IMAGE BY PHOTOS.COM

India is Third Largest Smartphone Market

India's smartphone market grows a massive 163 percent in Q1 2013

ACCORDING TO a new report by Strategy Analytics, India has pushed past Japan to become the world's third largest smartphone market in the first quarter. China and the United States of America remain the top two global markets and the report noted that this is the first time India has moved up to the third place ever.

The SA report documented a 163 percent increase in sales of smartphones in India in the first quarter of 2013, compared to the average 40 percent growth globally in the same period.

The report confirmed that this increase is due to improved distribution system of Samsung, Apple and Micromax.

Although Samsung and Apple remain the most sold brands, the report revealed that it is Indian brands like Micromax, Spice and Karbonn that have led to India's increase in the global smartphone share. These Indian brands have grown at a rate of 200-500 percent annually.

India also has a large number of smartphone micro vendors like Lemon Mobile which has reportedly seen a tremendous 1,000 percent growth, year on year. Other smaller palyers are also witnessing a healthy growth in the smartphone market.

DATA BRIEFING

11%

Was the fall in shipments of PCs in Q2 of 2013

IMAGE BY PHOTOS.COM
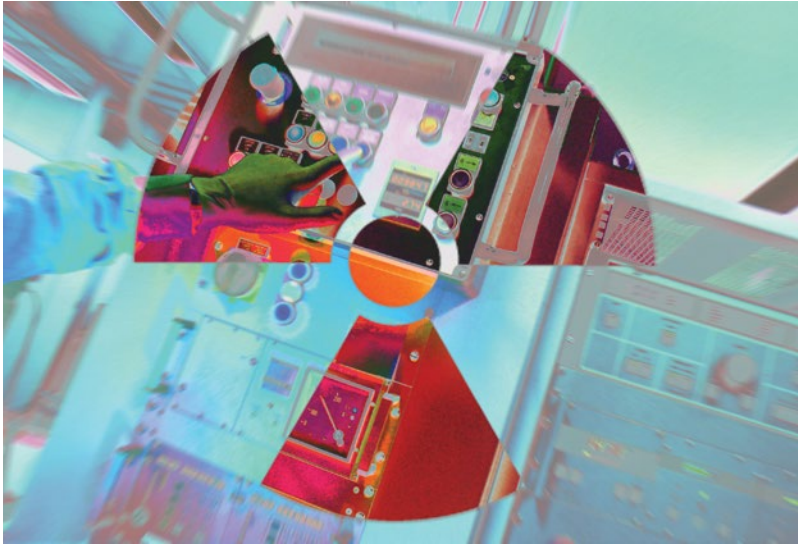
Marketing Automation Crucial To Businesses Will help users develop a taste for marketing

MARKETING automation is becoming a business imperative for attracting and keeping customers, and is central to the long-term survival of the modern enterprise, finds Ovum. The global analyst firm predicts that over the next six years a critical mass of businesses will make a leap of faith to invest in marketing automation, as internal pressures to automate marketing and fears of competitive disadvantage grow.

New research from Ovum's Digital Marketing and Connected Customer practice reveals that a cadre of enlightened CEOs and CMOs will drive the digital agenda and adoption of marketing automation. "Marketing professionals that ignore the significance of automation in the face of stakeholder pressure to be accountable, measurable, and transparent do so at their own peril," warns Gerry Brown, senior digital marketing analyst at Ovum. "Automation can provide a much-needed boost to marketing's credibility. It can change the common perception of marketing being a cost center to becoming a valued source of incremental revenue, profit, and customer loyalty. According to the report, users will develop a taste for marketing innovation using marketing automation technology tools.

THEY SAID IT **TONY FERNANDES**

Fernandes, who is about to launch an airline in India partnering the Tata group, is known to be as outspoken as he is focused on low costs. At a press gathering held recently, he didn't disappoint.

" Mr (Ratan) Tata is a fantastic guy. It is a fantastic experience working with him, although I have not gone to bed with him."

— *Tony Fernandes,*
AirAsia Group CEO

QUICK BYTE ON IT SPENDING

ILLUSTRATION BY PHOTOS.COM

"Global IT spending is growing, albeit cautiously" was the message shared by Gartner. While the analyst firm previously predicted a 4.1 percent growth in IT spending this year, they have lowered expectations to two percent for a total of $3.7 trillion

—*Gartner*

IMAGE BY PHOTOS.COM

SMBs More Supportive of External Social Tools SMBs are likely to utilise multiple external social tools for professional purposes

LARGE companies and SMBs use business social tools — defined as technologies that enable business collaboration and communication, such as intranets, video conferencing and social networks — in dramatically different ways, leading to very different selling motions and partner opportunities, according to a new research released by Microsoft at its annual partner conference at Houston, USA .

The study, conducted by the research firm Ipsos among nearly 10,000 end users at SMBs and large companies in 32 countries, found that, in addition to using solutions such as intranets and instant messaging services, SMBs are more likely to utilize multiple external social tools for professional purposes. Large companies, on the other hand, are more likely to deploy fewer, more prevalent collaboration tools.

Social collaboration technologies represent a growing opportunity for both large companies and SMBs to fully realize the

benefits of cloud computing through and all-inclusive approach to productivity," said Ramkumar Pichai, GM - Microsoft Office Division at Microsoft. "The new Office is more social than ever. With SharePoint, Lync and Yammer, Microsoft alone has the expertise, portfolio, capabilities, vision and insight to make the future for workplace collaboration a reality.

Other unique differences called out in the study include the following:

Although the top use for social tools in both large companies and SMBs is communicating with colleagues (selected by seven in 10 of all end users surveyed), those at smaller companies use social tools for a broader range of tasks, including communicating with customers, clients or vendors and researching customers, clients and competitors. In contrast, end users at large companies are more likely to use social tools for finding an expert of information within their company.

Barriers to adoption still exist across large companies and SMBs. For both groups, security concerns (71 percent of end users at large companies vs. 60 percent of SMB end users) and productivity losses (58 percent at large companies vs. 59 percent at SMBs) were identified as the top risks.

End users at large companies are more likely to say their IT department can be a barrier to using social tools (41 percent at large companies vs. 36 percent at SMBs).

Those at large companies are also more likely to say social tools are restricted at their workplace because of concerns about the company image (27 percent vs. 21 percent at SMBs) or data loss (25 percent at large companies vs. 22 at SMBs).

The consumerization of IT has changed the fundamental way in which businesses communicate, with enterprise social tools now following a 'bring your own device' model into the workplace," said Rebecca Sizelove, associate vice president, Ipsos Public Affairs. "However, there are distinct differences between how SMBs and large companies adopt these tools, and technology decision-makers still require a certain amount of education around the benefits social tools can provide. This creates opportunities for technology vendors to educate and sell to businesses of all sizes.

GLOBAL TRACKER

CRM

Customer Relationship Management (CRM) market will be at $36.5 billion by 2017, a significant increase from the $20.6 billion forecast in Q1 of this year

SOURCE: GARTNER

Govt Finally Gets Access To BlackBerry Communications

It was a long hard battle for the govt
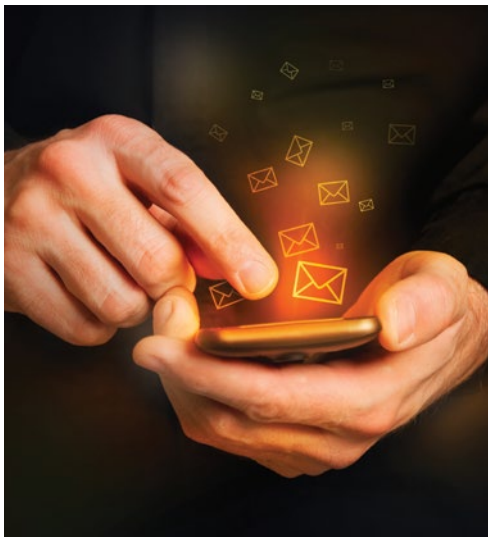
IMAGE BY PHOTOS.COM

THE STALEMATE between the Indian government and BlackBerry over allowing the former to intercept BlackBerry communication services is finally nearing its end.

According to reports, the Indian law enforcement agencies will soon be able to monitor e-mails and e-mail attachments real-time on BlackBerry services as well as messages delivered and read on BlackBerry Messenger.

According to Economic Times, which claims to have copy of an internal document of the Department of Telecom (DoT), "Baring a few minor points for improvement of viewers, the lawful interception system for BlackBerry Services is ready for use."

The government seems to have shelved the demand for having access to BlackBerry's corporate e-mail service rendered via the BlackBerry Enterprise Server.

BlackBerry says it had provided a solution to the Indian government that allowed the law enforcement agencies to have lawful access to its communication services, including BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email.

Despite BlackBerry's compliance, the state's access to data will not include Blackberry Enterprise Server. The firm highlights this in its statement to TNW the matter:

As informed earlier BlackBerry has delivered a solution that enables India's wireless carriers to address their lawful access requirements for our consumer messaging services, which include BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email.

The lawful access capability now available to BlackBerry's carrier partners meets the standard required by the Government of India for all consumer messaging services offered in the Indian marketplace.

We also wish to underscore, once again, that this enablement of lawful access does not extend to BlackBerry Enterprise Server.

Considering that BlackBerry has historically prided itself on its strong enterprise security, this was likely something that the firm fought hard to defend.

As end-users based in Metro cities in India reach saturation vis-à-vis adoption of most IT products and services, Tier-II and III cities are gradually reaching the next wave of technology adoption. IT Services plays a major role in this increased adoption. Consequently, major IT vendors and service providers are setting their sights on these India Tier-II and III cities for marketing their service offerings. IT Services account for a substantial 16 per cent of total small and medium business IT spending in India indicating its importance for future SMB growth.

While Product Support Services and Professional Services account for a huge majority; over three-quarters of the total IT Services market, Remote Managed IT Services (RMITS) has displayed a much faster CAGR and is fast becoming accepted as a mainstream service delivery model, according to AMI-Partners study - 2013 India SMB ICT & Cloud Services Tracker Overview .

The services and solutions segment in India is in a gradual growth-phase, especially within the mid-market segment. When considering which service provider to use both SBs and MBs state that scalability as well as total cost of ownership are important factors.

FACT TICKER

BI Revenue to Reach $113mn in 2013 CIO's are gaining a better understanding of BI implementation

INDIAN business intelligence (BI) software revenue is forecast to reach US$113 million in 2013, a 16 per cent increase over 2012 revenue of $98.1 million, according to Gartner. This forecast includes revenue for BI platforms, analytic applications and corporate performance management (CPM) software.

"Pressures from consumers, environmental policies, government and industry regulations, international standards of quality, and internal operational efficiency are forcing enterprises to improve their operations and processes to become both agile and efficient in a volatile marketplace,

" said Bhavish Sood, research director at Gartner. "These internal and external pressures are driving increased adoption of analytics solutions across the country."

Indian CIO's are gaining a better understanding of the non-IT competences required for successful BI implementation; however, a general lack of talent across all fields of information management in organisations will continue to be the critical barrier to their successful adoption of BA initiatives.

BEST OF BREED

IMAGE BY PHOTOS.COM

Technology Autonomy Boosts Profits

Profits would increase if employees could choose their own devices and applications By William Atkinson

Many IT and business executives say their company's revenues and profits would increase by an average of about 25 percent if employees were given the freedom to choose their own devices and applications, according to a just-released report by Blue Coat Systems.

The report, "Security Empowers Business: Unlock the Power of a Protected

Enterprise," is based on a survey of 1,910 IT executives and business executives from Europe, the Americas and Asia-Pacific. Half of the respondents are IT executives and half are business executives.

The Blue Coat report notes that, as the speed and functionality of different technologies rapidly improve, and their costs similarly decline, organisations' ways of working are changing substantially.

One way this phenomenon is manifesting itself in the enterprise is in the form of "technology autonomy"—the independence that employees and individual business departments seek in order to make their own choices about the technologies they use to perform their work.

Employees are increasingly demanding the freedom to use their own devices and mobile apps at the office, which is causing a disruption of IT.

"Users want the autonomy to choose their own devices, particularly mobile devices, believing that this will provide them with more efficiency and productivity," says Sasi Murthy, senior director of product marketing for Blue Coat Systems.

"They also want flexibility with the applications that they can use, even going as far as some cloud-based storage applications."

Over the years, however, many employees and departments have viewed IT departments as resistant to such autonomy, with some labeling their IT department as "The Department of No."

According to the results of the Blue Coat survey, though, this resistance appears to be steadily decreasing. The report notes that "such IT recalcitrance is fading fast. CIOs and other senior IT leaders in most organisations are now convinced that according greater freedom to business units to select and acquire the devices and applications of their choice will enhance business performance."

The key survey results include:

● More than eight in 10 of executives believe that technology autonomy is critical if their businesses are to grow and become more efficient.

● Fifty-four percent of executives believe

The Blue Coat report notes that, as the speed and functionality of different technologies rapidly improve, and their costs similarly decline, organisations' ways of working are changing substantially

their revenues would increase and 50 percent believe their profits would increase, by an average of about 25 percent, if employees were accorded the freedom they desire to choose their own devices and applications. Only 35 percent believe there would be no change in revenues and profits.

● The majority also agree that the benefits of technology autonomy would well outweigh the potential risks, provided that enterprises take security, compliance and cost requirements into account.

● The recent flexibility that IT departments have been offering related to technology autonomy is borne out by the fact that only four percent of business unit managers now believe IT merits the reputation as the "Department of No."

Along the same lines, pluralities of business heads and board members say that "IT is a genuine partner in the business."

● However, half of the respondents think that IT policies slow the business down. They say that restrictive IT policies hamper their organisation's ability to innovate, improve customer service, and boost overall revenue and profitability.

So, while there is a sense that IT has become more flexible, there is also a belief that additional flexibility is needed. "These days, there is a shift going on at the C-level in organisations to help continue this trend," says Murthy.

● IT management respondents broadly concur that IT should retain a major voice in decisions relating to mobile device provision, application selection, managing access to data, and accessing cloud-based services. Business management respondents believe there should be more collaboration about such decisions.

Of course, all of this raises the fundamental question: If IT allows more technology autonomy, how will the additional risk exposures be handled?

"IT is very concerned about this," says Murthy. "There is acknowledgement among respondents that at-will consumption is already occurring, so the 'cat is already out of the bag.'

For example, it is a huge concern for IT that users are storing data outside of the IT network." As a result, there must be appropriate ways to manage these security risks.

According to Murthy, one method is to be selective about what type of technology autonomy IT allows, such as limiting it to specific users, specific applications, and specific types of data. **C&L**

—This article was first published in CIO Insight. For more stories please visit www.cioinsight.com.

$288b

WILL BE THE SIZE OF WORLDWIDE IT OUTSOURCING MARKET IN 2013

Why Conferences Matter

Attending conferences is not only good for your professional development and career, but it enables you to be a more valuable resource By Larry Bonfante

I recently attended and contributed to a major CIO conference. I was fortunate to meet many new people and have conversations with many old friends and colleagues. This experience reminded me of a number of lessons that all of us can take away from these types of events.

● Regardless of how long you've been in the IT industry, you should never stop learning. I learned a great deal about gamification and crowdsourcing, which are two topics I was somewhat familiar with but hadn't given a great deal of thought to regarding how we could leverage them. The opportunity to unhook from work and attend a conference got my brain working on ways we can use these tools for our competitive advantage.

● You can always be a teacher. I had the privilege of being one of a dozen CIOs who were asked to act as mentors in a leadership session in which attendees could spend a half-hour at a table with three different CIOs (think speed dating for IT executives... ha ha!). It was tremendously rewarding to share some thoughts and lessons with these talented IT executives and see them become inspired by this new knowledge, which, I hope, will support their leadership development.

● Networking is an important thing to do, but as I always remind my coaching clients, it is less about being the life of the party and more about being genuinely interested in what other people are doing and finding ways to add value for them, as opposed to looking for ways that they can help you.

● I had forgotten how inspiring it is to leave the day-to-day work behind and to focus on new ideas and perspectives. I see too many
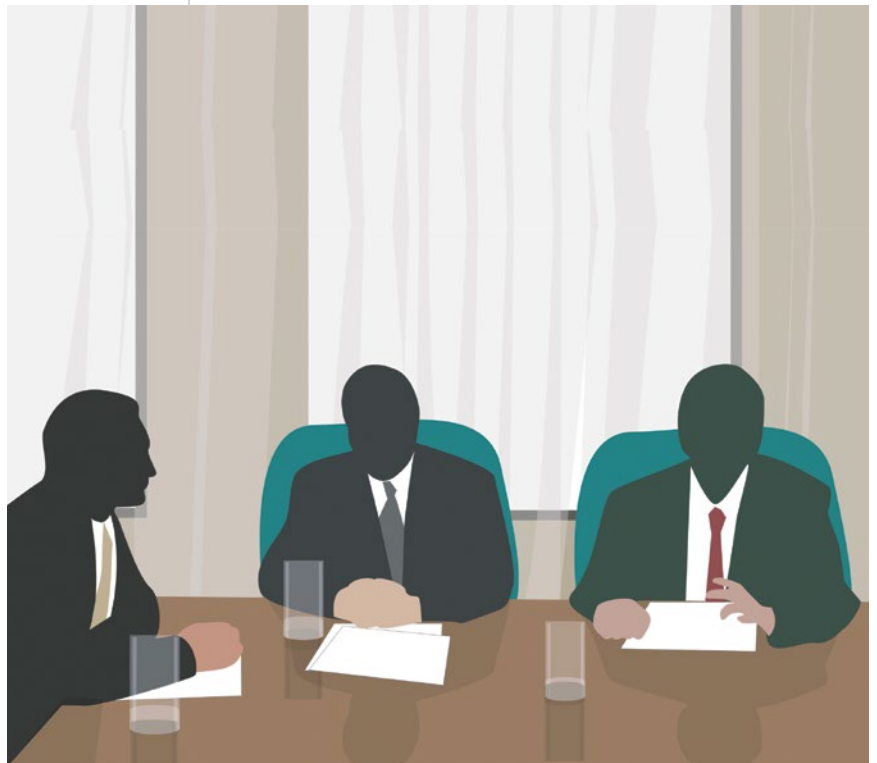
IMAGE BY PHOTOS.COM

Your professional development needs to be a top priority, and no one will care more about investing in it than you do

people at conferences spending their time talking on their iPhone, "putting out fires." I feel very fortunate to have a talented team who is more than capable of keeping the ship afloat, affording me the opportunity to learn new things and bring back different ideas and perspectives for the team to consider.

- Finally, a change of scenery is sometimes a healthy way to shake off the rust and make you feel re-energized and refocused. I'm reminded of Jimmy Buffett's song "Changes in Latitudes, Changes in Attitudes." Sometimes it's just good to leave behind the usual grind to get a new view on life.
- We all face the same challenges, and having a community to support each other and learn from each other is an invaluable resource.

When was the last time you attended a conference or workshop? Are you "too busy"? Prioritising your professional and leadership development is not only good for you and your career, but it also enables you to be a more valuable

$36bn

WILL BE THE SIZE OF GLOBAL SEMICONDUCTOR MANUFACTURING MARKET IN 2013

resource to your organisation. Many people spend more time planning their vacations than they do planning their careers. Your professional development needs to be a top priority, and no one will care more about investing in it than you do. **C&L**

—*Larry Bonfante is CIO of the United States Tennis Association and founder of CIO Bench Coach, LLC, an executive coaching practice for IT executives. He is also author of Lessons in IT Transformation, published by John Wiley & Sons. He can be reached at Larry@CIO-BenchCoach.com.*

—*This article was first published in CIO Insight. For more stories please visit www.cioinsight.com.*

The Fracturing of Corporate IT

The traditional IT organisation is disintegrating but will re-emerge in the IT ecosystem By Rajiv Sodhi

One of the biggest threats to corporate competitiveness is a shortage of key skills, and nowhere is that risk more acute than in the corporate IT organisation. By 2015, less than 25 percent of the current IT workforce is estimated to remain in stand-alone IT roles, according to analysis by the Corporate Executive Board. And top tech talent will migrate to the best opportunities, more likely working for a technology-centric organisation than for an enterprise IT organisation.

As a result, we will soon witness the beginning of the end of the IT organisation as we know it, but not the end of the modern enterprise's IT demands. Businesses will need more highly skilled technical talent in the future than ever before, as corporate systems grow even

more complex and critical. Consumption of data—structured and unstructured, internal and publicly available—will increase. Real-time and actionable analysis of that data will become a business requirement. And employees will demand access from

Customers who fail to change will fall behind their business rivals

anywhere on any device. Meanwhile, IT organisations once built on the foundation of servers, mainframe computers, software and human resources will reduce their dependence on all classes of technology assets.

The skills of the average corporate IT prowork. And customers who fail to change will fall behind their business rivals.

To get an idea of how this transformation will affect businesses, just take a look at a successful software company: It is asset light with little inventory. It is agile—and prepared to change tools or processes rapidly. It operates as every successful business soon will—as part of a well-oiled digital ecosystem.

Ultimately, this new model will be welcomed by traditional enterprise IT organisations currently struggling to meet the demands for cloud computing, analytics, mobility and social media. IT can let go of the old way of doing busi-

ness—being responsible for everything end-to-end—and embrace this new digital ecosystem of strategic partners, increased agility and lower costs. The business will dream up its vision, IT will offer technology options in support of that vision and a team of vendors will effectively deliver it.

The relationship will evolve from partnership to co-creation to co-innovation.

This transformation will not happen tomorrow, but we're now seeing the signs of it. Businesses that are early adopters will reap the benefits. The others, which idly wait and see, will miss out on them. C&L

—Rajiv Sodhi is senior corporate vice president of consumer, manufacturing, healthcare and public services delivery and chief customer officer at HCL Technologies.
—This article was first published in CIO Insight. For more stories please visit www.cio-insight.com.

Private Clouds Proving Their Popularity

The private cloud is the most popular model, with SaaS being the most popular form **By William Atkinson**

Private clouds are the most popular cloud deployment model, according to the new 2013 Cloud Computing Survey conducted by Palmer Research and QuinStreet Enterprise. Also, software as a service (SaaS) is the most popular form of cloud computing service used by the respondents, besting both infrastructure as a service (IaaS) and platform as a service (PaaS).

The survey is based on reports from nearly 350 IT professionals and executives who are involved in the cloud computing purchase process.

It found that 65 percent of respondents use or plan to use a private cloud. Forty-six percent of respondents use or plan to use a public cloud, and 19 percent use or plan to use a hybrid cloud. In addition, the private cloud seems to be growing at twice the pace of public and hybrid clouds.

Two reasons for the popularity of private clouds are security and privacy. That is, despite the best efforts of cloud computing vendors, and increasing adoption of cloud computing in recent years, concerns about security (mentioned as "extremely or very

Two reasons for popularity of private clouds are security and privacy

inhibiting" by 70 percent of respondents), privacy (69 percent), uptime (62 percent), and control of data (61 percent) remain the most likely inhibitors to adopting cloud computing services and applications.

In terms of types of cloud computing services, software as a service (SaaS) is the most popular form of service used by the respondents, with 78 percent of them using or planning to use it. Infrastructure as a service (IaaS) is second, with 60 percent of respondents either using or planning to use it. And platform as a service (PaaS) is a third, being used

by 24 percent of respondents, but with more than one-third say they are planning to use it in the future.

While SaaS is more than a decade old, and IaaS and PaaS are much newer, adoption of IaaS and PaaS is picking up quickly, with as many respondents planning to use them in the future as are planning to use SaaS.

The most surprising result is the growth rate of the private cloud and how this relates to the security and privacy concerns that have continued to exist for some time, says Mike Pastore, director of custom content for QuinStreet Enterprise and author of the cloud report.

"When you look at the top players in the public cloud, such as Microsoft, Amazon and Google, these are large and powerful consumer names," Pastore notes. "I would guess that most IT decision-makers trust their personal information to most or all of these companies. Yet, when it comes to business data and customer information, they see too much risk there." C&L

—This article was first published in CIO Insight. For more stories please visit www.cioinsight.com.

Stop being consumed by where you are...

...focus instead on where you want to be.

Are you at that stage in your career... when you start looking for something more. It could be a new direction, fresh focus or the next mountain to climb.

You've already come a long way, but it's time to aim for the top - the pinnacle.

But scaling the next mountain is a big stretch. You need new skills. You require new perspectives. You want to be a stronger leader.

The Pinnacle Programme will help you do all this - and more.

WE DON'T BELIEVE IN ORDINARY

WE BELIEVE IN YOU.

THE
LEADERSHIP
INSTITUTE

www.theleadershipinstitute.in

9.9 Mediaworx, B-118, Sector 2, Noida – 201 301, India   Tel: +91 120 4010999

CASE STUDY | **THERMAX**

Thermax Strengthens Information Security

CHALLENGE: Thermax was saddled with legacy infrastructure in the form of **traditional desktops.** While the company was **growing steadily,** the IT infrastructure was lagging behind

BY TEAM CIO&LEADER

Thermax is a Pune-based company that provides a range of engineering solutions to the energy and environment sectors. It has a global sales and service network spread over 21 countries and nine manufacturing facilities - five of which are in India and four overseas.

Legacy infrastructure was a bottleneck

Thermax was saddled with legacy infrastructure in the form of traditional desktops. While the company was growing steadily, the IT infrastructure was lagging behind. "Some of our traditional desktops had been in use for more than five-six years, and could not cope with new operating systems. This would have prevented Thermax from leveraging new technology," says Anil Nadkarni, CIO, Thermax Ltd.

Globally, the company has around 4,600 employees.

The other challenge faced by the company was that of security and control. According to Nadkarni, being an engineering company, Thermax's core intellectual property is engineering drawings. "These drawings have to be stored, protected and managed centrally. Similarly, as we bid for projects, we can't afford leaks. Securitising such data was a big challenge we faced," he says.

"As a company with a high concentration of engineers, our employees expect maximum output from any machine that they work with. Therefore, technologically, we needed to upgrade urgently," says Nadkarni, who manages a team of 30 people.

The solution that aligns with business

To overcome the challenges, Nadkarni realised that in the first phase, there was a need to replace 1,000 desktops. "We internally debated that even if we were to replace

1,000-1,500 PCs in one go, five years down the line we would again have the same challenges," he says. Therefore, Nadkarni decided to explore desktop virtualization as a credible option.

After getting the go-ahead from the company's management, Nadkarni initiated the stringent process of evaluating various solutions in April 2012. "We looked at both Citrix and VMware. To test all the critical applications, we invited both the companies to give us a PoC. One important feature that we wanted in the solution was flexibility. While VWware's VDI solution was a completely dedicated desktop, Citrix XenDesktop solution was both a shared as well as a virtual desktop," informs Nadkarni. The flexibility of the Citrix solution tilted the balance in its favour. As Nadkarni says, "I believe that if you are dedicating a desktop to one person, you are not fully utilising its power.''

On the infrastructure front, Thermax needed a system which would form the backbone of its transformed workplace, a system which would be capable of handling its entire business critical workload, which allows for ease of management and low consumption of power. Upon evaluating IBM and Dell, Thermax chose IBM for its unique solutioning and its capability to implement the solution end-to-end. "One of the major issues we envisioned was when multiple users would log into the system in the morning. This needed a lot of storage performance for a short while, which would have increased the pricing, and the price per user. However, with FlexSystems V7000 storage design, offering SSD based easy tiering, we could use a few high performance disks to achieve the performance, without impacting the price. I feel this was the fine point that made us go for IBM" explains Nadkarni. "We chose the IBM FlexSystem as the platform of the future to build our requirements on.''

Thermax deployed IBM servers with 10 eight-core CPUs, and two six-core CPUs. The company has 30 Terabytes of NAS storage and 6 Terabytes of SAN storage. For its storage infrastructure, Thermax went for the latest Storwize v7000, which is known in the industry for its technology on realtime compression and storage virtualization.

Making Thermax BYOD ready

Once Thermax decided to deploy Citrix XenDesktop, the actual implementation of the solution started in the second week of August 2012. "By the end of August we had rolled out 50 users as a test. We watched them for about 15-20 days. We received a fairly good response and there was nothing to complain. The implementations went smoothly. The solution was then rolled out at two of our manufacturing facilities – Pune (500 users) and Baroda (250 users)," Nadkarni says.

By the end of October, Thermax had 750 people live on Citrix XenDesktop. According to Nadkarni, he received a lot of support from the technical team of Citrix and the implementation team of IBM. "We had a great experience working with Citirx and IBM. Their technical team provided valuable know-how relating to server configuration and server sizing." he says.

COMPANY DASHBOARD

◤ **COMPANY:**
Thermax India

◤ **ESTABLISHED:**
1980

◤ **HEADQUARTERS:**
Pune

◤ **SERVICES:**
Chillers for large scale air conditioning units, steam generators, and boilers

In this first phase, barring the engineering applications, Thermax has made all the non-engineering applications (such as ERP, instant messaging, HR application) available through Citrix XenDekstop. "The biggest advantage of the deployment has been that my organisation has now become BYOD (bring your own device) ready. Today, we have about 20 tablet users who log in from anywhere. Such anytime- anywhere access has enormously improved the company's decision-making. With the success of this project, we are seriously contemplating not to give desktops or laptops to our employees from now on. They can bring their own computers and tablets to work. I am less worried about the security issues now," says Nadkarni.

"Citrix XenDesktop has also given us the advantage of managing data centrally, thereby giving us the power of enhanced security and control," he says. Encouraged by the benefits from the Citrix solution, Nadkarni is now expanding the deployment to the rest of the organisation. "Out of the 4,500 desktops in India, we have already migrated 800 users onto the new solution. We want to extend it to 1,000 more employees within the next 5-6 months." C&L

CFO Who became a CIO

In his illustrious career,
V S PARTHASARATHY
has been a CFO, controller-financial planning,
headed international ops of a subsidiary,
and acquired companies abroad.
He has also managed IT.

BY YASHVENDRA SINGH

Design by: SAMEER KISHORE   Photos by: JITEN GANDHI

Walking the Talk

Been there, done that. V S Parthasarathy has donned several roles in his leadership journey. Leading from the front, he has proved to be successful in each of the profiles   BY YASHVENDRA SINGH

There are few CIOs in India who have shouldered such diverse responsibilities and played such varied roles as V S Parthasarathy, Group CIO, EVP - Group M&A, Finance & Accounts, Mahindra & Mahindra. He is also the Member of Group Executive Board, M&M Group. At various points in his career, he has also been the CFO, and the Head of International Operations.

He describes his journey to the top in his own words as a connect to his childhood journey, which had very lasting impressions in his life.

"I was born in Chennai. I recall when my parents were staying in

Mehboob Nagar in Hyderabad; since then we moved from place-to-place with an average time of three years in one location. Within the three years, we used to have an average time frame of one year per house."

"*Naya Sheher* would mean stay in a '*saray*' initially, then a rented house, before actually getting into our own quarters. So by the time we settle into the one house with parents and four of us (brothers-sisters), it would be time to shift to the next," he recalls.

This life of a gypsy gave Parthasarthy (Partha) the ability to make new acquaintance, friends; ability to adapt, and face ambiguity. In fact, he developed an empathy fo the gypsy community, which he started to represent.

"Going to new fields, new geographies helped me a lot later in life. My career also went on a similar path with the roles migrating around every three years," he avers.

Earlier in the career one of Partha's friends, who had joined Modi Xerox (now Xerox India), was helping the company set up a branch in Ahmedabad. The division was in need of a branch CA Head. Partha was interviewed for the position but did not get hired because his CA results were not out yet. It was only when he cleared the CA examination that he quit his AF Ferguson job in Mumbai to join Modi Xerox in Ahmedabad.

Partha proved his mettle at Modi Xerox within the very first year. He

achieved a target of more than 100 percent and was awarded the best credit performer in 1987. He became a part of a very select club called 'Honorary Club'. So, what was Partha's mantra of success?

"I was able to achieve the target because of three very important things – enthusiasm of the team, detailed planning and excellent team support. Not to forget, a bit of luck," he avers.

Modi Xerox then decided to send Partha to Lucknow, Uttar Pradesh (UP), to expand the operations in the state. He recalls an incident with his boss just prior to relocating, when Partha's boss had told him that the next time they meet, Partha would have become his superior in the company. He had also shared how much he enjoyed working with him and that he would root for his success.

"I thought it was a very poignant way to look at things, and my boss really meant what he said. Those words have stayed with me throughout my career," Partha says wistfully.

When he was sent to UP, Partha was told that he would not survive for more than a three months. However, three-and-a-half years had passed before he moved out of UP during which time UP went in the Xerox's League table from the bottom to the top of the table.

At Xerox, Partha underwent a 'Leadership Through Quality' programme that left an indelible impression on him.

The programme was kicked off by Xerox CEO David T Kearns in the eighties. It emphasised on quality in everything that was done.

"The big Q rather than just push for quality," says Partha. "The course had a great impact on me. It taught me to do everything the quality way. The programme made us believe that one can achieve leadership in business by applying the quality principles."

It was the learnings that Partha imbibed during this leadership programme that helped him take Xerox in UP right to the top.

"The quality principles had taught me some interesting problem solving techniques. Root cause analysis brought some facts to the surface. The problem in UP was that people were focusing on collection only and ignoring controls. There was ineffective F&A leadership, and low business partnering," he says.

Giving an example, Partha says, "Rather than doing billing based on actual billing meter, adhoc billing was done based on assumptions; leading to customers not paying."

Deploying simple things helped. Tough actions, leading by examples, and forming an effective credit team made all the difference.

Continuing with his gypsy lifestyle, Partha moved to Kolkata in 1990 as Regional Controller and Operations Head at Xerox. In 1994, he was moved to the Xerox head office in Delhi as Controller-Financial Planning and Analysis (FP&A). From 1994 to 2000, he continued to be the FP&A head, and was also the CFO for two units of the company.

This was Partha's first stint as the CFO. However, he already had the skill set needed for the role.

"The skills required as a Controller were pursued in the CFO role wherein 'enabling or empowering team', 'leading from front' helped me. The expertise widened and I got more involved beyond finance and accounting functions," he recalls.

It was during year 2000 that Partha met K J Davasia, the then President and Executive Director of the Farm Equipment Sector (FES) at M&M. At that time, he had no plans of moving out of Xerox.

But M&M's Davasia was persistent. In a bid to attract him, he told Partha, "How would you like to make an Indian company the world's number one in manufacturing tractors?" Partha rose to the bait and agreed. "Mr Davasia asked me to join in and be a part of the company in its journey to greatness. It was a great statement from a great man," recalls Partha.

The Road Ahead

What is the way forward for CIOs?

"CIOs of today are standing at the cross roads of a historical path. They need to choose to be wise and work in peace; else would 'rest in peace'. CIOs should have business knowledge and the aspiration to be on the board. The world has witnessed Chief of Finance, Chief of HR, Chief of Manufacturing becoming a CEO in the past. It's the CIO's turn now. The CIO should think like a customer and act like a CEO. 'Enable-Enhance-Engender' is the mantra that I have given to my IT Team. "Engender – otherwise you are in danger" is what I advise to the fellow CIOs.

It will be an IT-driven business in the near future and keeping the organisation 'Future Ready' will be the challenge for the CIO. But technology is moving by leaps and bounds, so to catch its speed and prepare an agile organisation is not an easy task for the CIO. Going forward, its cherish or perish scenario for the CIO. While I have already played the CEO role while heading the international operations, it is the forthcoming Group CFO role, which I will take over from my current portfolio that I am looking forward to now."
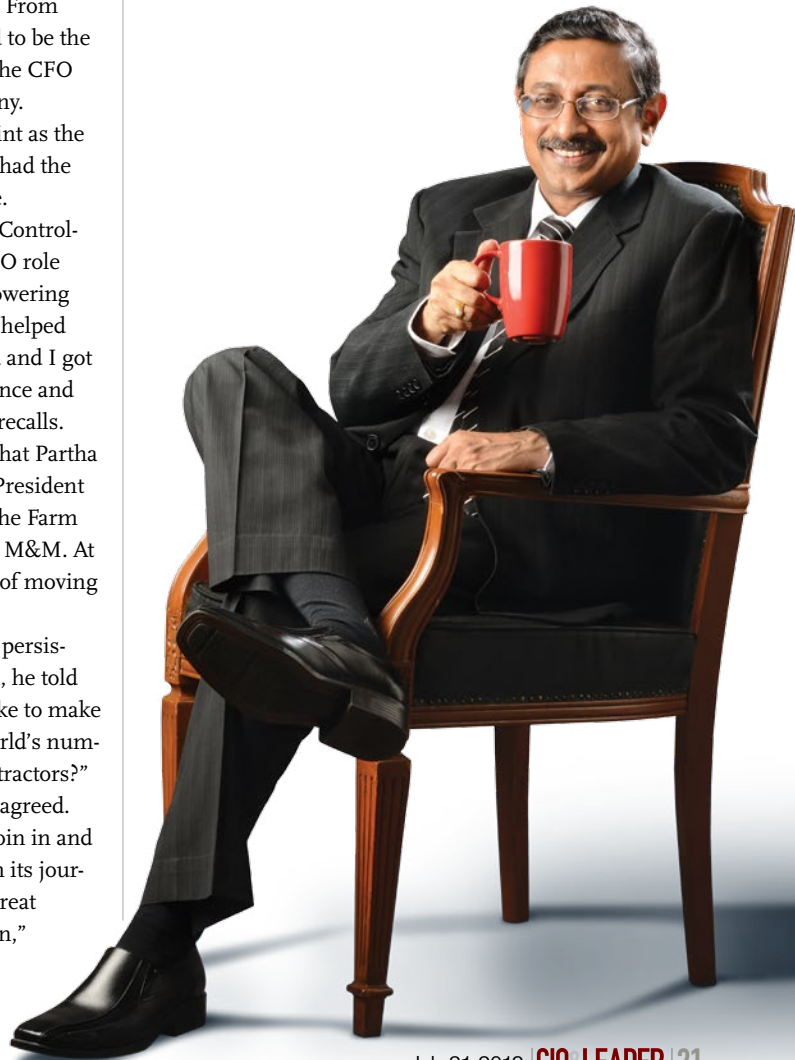
So Partha, never one to shy away from a challenging responsibility, made his next big career move. After 14 years with Xerox, he joined M&M's FES in February 2000 as Head of Performance Management and Organisational Development (PMOD) and Head-IT.

However, aligning people within the IT team was a big challenge. Partha had to build the trust of his team members, offer them a vision and ask them for their support to make a big change.

This is where the Leadership Through Quality approach again came to his rescue.

"I had to take away the fear in them. The only thing that made the difference was communication, communication and communication," he says.

This was another landmark in Partha's career as he was given the responsibility of handling the IT of FES. Leading from the front, Partha, leveraged IT for successfully growing business.

In 2001, he was instrumental in choosing a supply chain solution from SAP that helped the company reduce inventory in the supply of finished goods, improve order fulfilment rates, and reduce demand fulfilment time, which turned out to be the first supply-chain implementation in the Asia-Pacific region. Under Partha's leadership, FES was the first division to implement a business warehousing solution.

In 2004, Partha was made Head of International Operations where he was responsible for FES' worldwide operations, excluding India. He played a key role in M&M's acquisition & joint venture of China-based two companies to set up Mahindra China Tractor Company Ltd. Business in the US increased from 1,000 tractors to 10,000 tractors.

In 2008, Partha was called to the Mahindra headquarters and appointed as Head of Mergers and Acquisitions (M&A). Later he got a group role in IT and Finance. In 2010, he was made the Group CIO.

So how did he take to this daunt-

ing task of managing both IT and finance?

"Right since Xerox, IT was integral in my roles. During my tenure, the first offshore development center came up in India for Xerox. Even while joining FES as head of Performance Management & Organisational Development, I opted for IT as a part of my role. I strongly believed that without IT, it would be difficult to drive the change in people. So while in head office, it came as a natural profile for me with a bigger role to play," says Partha.

Not only did Partha handle the role of a CIO, he also successfully steered the M&A strategy for the company. Under his leadership, the M&A team executed over 60 transactions and 25 acquisitions around the world.

"I just basked in the glory. It was my team that helped us execute these initiatives," Partha quips.

Life as a CIO

M&M is a big conglomerate. With 10 business sectors present across 18 industries makes the role of Group CIO more difficult. Each business sector charts its own course, makes its own strategy, has its own IT which reports to the business and does not have a functional linkage right upto the top. So the decision making is near this and IT is part of it. The challenge remains of making a common IT system in a federated environment.

According to Partha, "You do not have authority, you are only a story teller. Its like being driven in a plane where you are not pilot nor co-pilot. But you need to navigate the plane with a pilot who can overrule you."

So how did he manage the IT of such a diverse group?

"The first thing to start with, is taking a deep dive and understanding the needs of the business and people. There is a three-tier IT ecosystem in place across the group -- Strategic Leadership Council, Technology Leadership Council, and Cross Functional Teams. The last one helps

" I WAS ABLE TO ACHIEVE THE TARGET BECAUSE OF THREE VERY IMPORTANT THINGS – ENTHUSIASM OF THE TEAM, DETAILED PLANNING AND EXCELLENT TEAM SUPPORT. NOT TO FORGET, A BIT OF LUCK "

—V S PARTHASARATHY

decide on the various initiatives, either specific to a sector or for the group. I would generally have a 'nose in and hands out' role in all these," he says.

So what was the toughest decision that he took as the CIO?

"At M&M, the consolidation of SAP across all the companies (dubbed Project Harmony) was the toughest decisions to take. Selling the solution to each of the companies, take their buy-in and finally to get over 90 percent of the companies on the board," he says. The left out companies were either too nascent in their life cycle and could not afford or some were to evolve into something else and it would cost them huge amount of time and effort to join.

There was a huge risk of bringing all the companies on a single instance (common server, storage, computing, backup & DR) and still keep it running 24x7. Extra investment was done for a DR to take care of this which included NearDR, FarDR alongwith the Tape Backups.

In Person

With his excellent domain knowledge in finance, coupled with in-depth business perspective, Partha is a role model and a macro manager who always trusts his team. During challenges, his calm approach, direction and empathy for the team proves to be an asset. He has always promoted lateral thinking as well as the ability to engage and influence internal stakeholders.

Beyond reading and listening to music, he loves mentoring the young blood and setting smart goals for them. Entrusting the people and developing them to do the unthinkable, has been something which he has pursued and his team mates have experienced it. He does not stop looking only at corporate activities, but goes beyond to help the society to benefit from the IT knowledge of the team. He put forth a dream to his team to pass on the latest IT knowledge to the next generation so as to transform them into tomorrow's IT professionals depending on their level of interest. **C&L**

"RATHER THAN QUANTITY OF TIME, IT'S THE QUALITY TIME HE SPENDS WITH US AT HOME THAT MATTERS"

— JAYASHREE PARTHASARATHY

"Partha is a self-critic"

In a candid discussion with CIO&Leader, **Jayashree Parthasarathy**, the better half of V S Parthasarathy, provides a sneak peek into his personal life

Q Is Mr Parthasarathy able to strike the work-life balance? How?

He is able to spend quality time with me and our sons. We find time to go out for movies, have dinner out once a fortnight. We also take regular short bust holidays even in the hustle and bustle. He laughingly keeps telling his

friends that "I have seen more airports but my wife has seen more cities". His organisation also encourages taking me for office programmes or events and that allows me to travel without compromising my office priorities. He would say he is not able to strike the balance considering his busy and late schedules in office, but rather than quantity of time, it's the quality time he spends with us at home that matters.

Q Do his leadership abilities reflect in his personal life as well? Please give an example.

He is humorous and he keeps joking "I am the boss of my house and I have permission of my wife to say so", but that's not true. At home we are a team. His stronger quality in office is team work and joint leadership, which equally reflects at home as well.

Q What qualities do you admire in him? On which fronts do you think he needs to improve?

Dedication, Simplicity, steadfastness are the qualities to name a few. Ability to have fun and enjoy even small things in life is highly admirable. Humorous at times, he is always being there without being intrusive. He sees more faults in himself and is a self-critic; which I would like to see less of.

Q How does he spend a typical day at home?

Being a voracious reader, he loves to spend the day reading books. He is very fond of poetry and also sports. So during free time, he keeps himself busy in books and books.

Q How does he deal with work-related stress/pressure?

He is able to keep work separate from home. So he never ever brings work home. Neither do we discuss office at home. The office mode gets switched off the moment he comes home. He would watch TV to get rid of the office mood and then he is 'present' at home. **C&L**

"He wears multiple hats"

Richard D'Souza, Head IT Projects & Central Support, Mahindra Group, admires V S Parthasarathy for the different roles that he plays, and believes he has what it takes to be a true leader

How would you rate Mr Parthasarathy on a leadership scale of 1-5 (1 being the lowest and 5 the highest)? Please give reasons for your choice.
I would rate him as 5 on the leadership scale. The reasons are -- he propels the team into a high growth trajectory, is a great leader who is always leading the team through his words and actions, with his strong networking skills he easily builds collaborative relationships, and most importantly he possesses excellent people management skills.

How is he as a boss? How is his management style?
He has been a good boss to me. He comes across as a great mentor, who guides and prods you on to deliver. He is a people's person who can easily spot talent. He uses their potential to help them deliver their best.

What are the top two-three qualities that you admire in him?

Having worked with Partha, I have come to know that he has powerful insights, networking ability and strong people management skills.

Can you recall any incident where Parthasarathy's leadership abilities came to the fore?
M&M launched one of the world's largest Big Bang SAP Project "Harmony". Parthasarathy regularly reviewed the project and at the time of "Go Live" he went along with the team to meet various business leaders and only when he was convinced he declared the project, "Go Live".

What are his shortcomings?
He wears multiple hats; hence time is always a constraint. We need to have an excellent elevator pitch to quickly get the message across. However, his grasp on varied subjects enables him to understand issues and situations better. **C&L**

CIO&LEADER

"Management is doing things right; leadership is doing the right things."

— PETER F. DRUCKER

CIO&LEADER This special section on leadership has been designed keeping in mind the evolving role of CIOs. The objective is to provide an eclectic mix of leadership articles and opinions from top consultants and gurus as well as create a platform for peer learning. Here is a brief description of each sub-section that will give you an idea of what to expect each month from *CIO&Leader:*

28 LEADING EDGE

An opinion piece on leadership penned by leadership gurus. Plus, an insightful article from a leading consulting firm

27 TOP DOWN

This feature focusses on how CIOs run IT organisations in their company as if they were CEOs. It will comment on whether IT should have a separate P&L, expectation management of different LoB heads, HR policies within IT, operational issues, etc. This section will provide insights into the challenges of putting a price on IT services, issues of changing user mindset, squeezing more value out of IT, justifying RoI on IT, attracting and retaining talent, and competing against external vendors

32 ME & MY MENTEE

Cross leveraging our strong traction in the IT Manager community, this section will have interviews/features about IT Managers and CIOs talking about their expectations, working styles and aspirations. In this section, a Mentor and a Mentee will identify each other's strengths and weaknesses, opine on each other's style of functioning, discuss the biggest lessons learnt from each other, talk about memorable projects and shared interests

36 SHELF LIFE

A one-page review of a book on leadership

Provide Customers With Maximum Choice

VC Gopalratnam, CIO and VP IT, Cisco, talks about the need for customer delight

IMAGE BY SUBHOJIT PAUL

TECHNOLOGY IS evolving everyday and a CIO has to always be on his toes. He has to come up with innovative solutions to attract customers. Today, we can no longer be glued to a particular technology. We rather be open to strategic changes.

The most important thing to consider is what will be the most valuable proposition for the organisation. Being a CIO, I get the chance to implement the best of the technologies in the organisation.

But the trick is to know what will be beneficial for the company and implement only those technologies. I always tell my team the importance of innovation and the fact that if we can develop solutions which can make the customers happy, we will be the ultimate winners. Customers have the choice of picking any vendor, so we need provide the customers the best possible offering. Another important thing for us is to be able to adapt to change.

Some of the trends that are making inroads today are big data, analytics, private, public and hybrid cloud and mobility. We are in constant touch with enterprise CIOs to understand their needs. Accordingly, we work towards developing solutions that would help them. Another important thing is to address the security concerns of the enterprises as we feel it is one of the priority of the CIO.

We, at Cisco, try to offer the best of the services in these domain to the customers. IT-as-a-Service is the order of the day and going forward only those vendors will succeed who can provide the best services to the customers and works with them as strategic partners. Customers want trust and vendors can gain that trust by helping them overcome the pain points.

It is also critical for the the vendors to benchmark themselves. They have to sell, manage, understand the competitive trends and they need to have a service catalogue for the customers, because the best way to retain customers is to offer them flexibility of choice. **C&L**

– As told to Atanu Kumar Das

The do-or-die questions boards should ask about tech

Board members should raise nine critical questions when discussing technology strategy with IT and business managers **By Paul Willmott**

SOME ORGANISATIONS are creating new technology forums, building the expertise of corporate directors, and strengthening IT governance—all with the aim of allowing boards to guide management by asking the right questions about technology. But what are the right questions at a time when digital technologies are beginning to disrupt industries and mastering these technologies may be the key to long-term survival and success?

The particulars of each enterprise's situation will, of course, determine the focus of the discussion and the detailed questions to ask.

However, across industries, every corporate director—IT savvy or not—will benefit from reviewing the following questions as a starting point for shaping a fruitful conversation with management about what the company needs to do to become a technology winner.

1. How will IT change the basis of competition in our industry?

Technology is making boundaries between industries more porous and providing opportunities for attacker models. For example, in the banking industry, online consumer-payment products such as Square—a mobile app and device that enables merchants to accept payments—are challenging traditional payment solutions. Free Mobile, a French tele-communications attacker, has captured significant market share by offering inexpensive mobile voice and data plans, in part by offloading some of its traffic onto the home Wi-Fi access points used by its broadband customers.

For incumbents in many sectors, technology is becoming an arms race. Companies are harnessing technologies such as social media and location-based services to reinvent the customer experience and capture market share.

Questions to ask:
- Who are our emerging competitors?
- How is technology helping us win against traditional and new competitors?

- How does our customer experience compare with that of leaders in other sectors?
- What will our customers expect in the future, and what will it take to delight them?
- Do we have clear plans for how to meet or exceed their expectations?

3. Do our business plans reflect the full potential of technology to improve our performance?

Technology expenses can be high, but they are relatively small compared with their potential to boost the operating performance of the business.

Technology can improve business performance by driving revenues (for example, by using big data for cross-selling in digital channels), reducing overall costs (for instance, by automating end-to-end processes), and lowering risk costs (for example, in insurance, by using social-media data to aid risk calculations). Technology can also have a negative impact on performance (for instance, by reducing margins given increased transparency about pricing in the market).

By seizing the opportunities and mitigating the threats, companies can dramatically improve their performance.

One retailer has doubled revenue growth by investing in the digital channel. A bank is targeting a 10 percent reduction of operating costs through automation of end-to-end processes.

Ultimately, the strategy that emerges from an assessment of opportunities and threats should be an integrated plan that shows how the business will beat the competition using information over a multi-year horizon, not simply a revised annual IT budget. With the right agreement on the scale and scope of the opportunity and threat, the level of investment in IT becomes an outcome rather than a constraint.

Questions to ask:
- Has the P&L opportunity and threat from IT been quantified by business unit and by market?
- Will our current plans fully capture the opportunity and neutralise the threat?
- What is the time horizon of these plans, and have they been factored into future

- How can we use technology to enter new markets?

2. What will it take to exceed our customers' expectations in a digital world?

Customers are being educated by e-commerce leaders like Amazon and Apple to expect an ultraconvenient experience, personalised in real time.

Attackers in many industries are differentiating themselves from incumbents through convenience and service. Digital finance company Wonga, for example, settles loans in 15 minutes.

As a result, customer expectations are rising quickly. Simply meeting these enhanced expectations can be a major effort for organizations that were not born digital.

For instance, retailers may need to step up their development of digital channels. Banks, insurers, and telecommunications players may need to automate end-to-end sales and service processes so that customers can interact with the company in real time in an error-free digital environment. The bar is high for delighting customers in a digital world.

Often, doing so requires investment in sophisticated big-data capabilities that use social, location, and other data, for example, to attract potential customers to product promotions at stores in their vicinity.

Questions to ask:

financial projections for both business and IT?

4. Is our portfolio of technology investments aligned with opportunities and threats?

The portfolio should clearly reflect the business opportunities and threats at stake. It also needs to be dynamic—executives must avoid the temptation to reuse the allocations from the previous year's budget without a close review. Companies should balance short-term

> ## "Leading businesses are continually using IT to improve business agility"
>
> **—Paul Willmott**

P&L opportunities (for example, upgrading digital channels), medium-term platform investments (such as customer databases), and carefully chosen longer-term bets (for instance, piloting new, digitally enabled business models).

Regular, often quarterly, portfolio rebalancing is needed, as assumptions can change quickly.

Many companies, for instance, recently cut investment in the Internet channel, as customers have switched to mobile apps. The portfolio should also be managed to keep execution risk in an acceptable range. On average, large IT projects run 45 percent over budget and seven percent over time, while delivering 56 percent less value than predicted.

These risks can be managed by monitor-

ing the portfolio carefully and deploying effective processes that assure value will be created.

Questions to ask:
- How well is our IT-investment portfolio aligned with business value with regard to opportunities and threats?
- How well does the portfolio balance short-term and long-term needs?
- Do we have effective value-assurance processes in place to mitigate execution risk?

5. How will IT improve our operational and strategic agility?

IT has a significant effect on operational business agility (for example, time to market for new products), as well as on strategic business agility (for instance, the ability to extract synergies from an acquired business or the ability to connect systems to a distribution partner).

Leading businesses are continually using IT to improve business agility. For example, one logistics operator has created a control room where the location and condition of assets such as rolling stock can be viewed in real time, enabling a swift response in the case of equipment failure.

Business agility is underpinned by the agility of the IT function itself—its ability

to design and implement changes to systems rapidly at low cost and risk. IT agility can be increased by changing the systems landscape (for example, by reducing the number of systems), improving data quality (for instance, by creating enterprise data standards), optimising IT delivery processes (for example, by applying lean-management techniques), and building flexibility into sourcing arrangements (for instance, by buying processing capacity on demand in the cloud).

Leading businesses measure and manage both business and IT agility, ensuring that the business can respond competitively.

Questions to ask:
- How does our business and IT agility measure up with that of our competitors?
- How do our IT plans increase our business and IT agility?
- Are our sourcing relationships increasing or reducing our agility?

6. Do we have the capabilities required to deliver value from IT?

Technology alone delivers no value. It's the combination of a clear strategy, the right technology, high-quality data, appropriate skills, and lean processes that adds up to create value.

Any weak link in this chain will lead to poor value delivery from IT.

For example, one telecommunications company introduced a new IT system to support cross-selling in stores but found that revenues didn't increase until the quality of customer data was improved, staff were trained in how to have the right conversations with customers, and sales processes and incentives were realigned.

Leading organisations actively assess their capabilities in these dimensions and target their weak spots. One bank, for example, recently created a group data-services team to improve the quality of data across the enterprise.

In many sectors, a shortage of IT-literate talent in the business is creating a bottleneck.

Contrary to popular belief, the majority of executives can, with the appropriate training, learn how to manage value from

IT. But capability building must start at the top.

Some companies have put their top 200 managers through IT boot camp as a way to start the process.

Questions to ask:

- Do we have the capabilities needed to drive full value from our existing IT systems?
- What are the weakest links in our capabilities?
- Do we have enough IT-literate executives?
- What is our plan for upgrading capabilities?

7. Who is accountable for IT and how do we hold them to account?

In most organisations, accountability is clear for functions such as finance and human resources. In HR, for example, performance can be tracked using a scorecard of intuitive business metrics such as attrition.

But accountability for IT is not always so well-defined. So-called shadow IT functions—such as IT developers hired into the marketing department to build social-media apps—can sometimes be out of reach of the core IT function. The emergence of roles such as the chief digital officer and chief data officer can further confuse the picture. Moreover, the IT function can't be held solely accountable for delivering value from IT.

Lower process costs, for example, benefit business units and functions other than IT.

IT can also prove hard to measure. All too often, volumes of technical data are presented instead of a limited set of intuitive, business-relevant metrics.

Measures of IT productivity or the bottom-line value delivered by IT are seldom available.

Leading organisations define a clear IT operating model, which determines exactly who is accountable for IT activities such as developing apps, managing data quality, or implementing IT solutions in business processes.

The operating model must be aligned with business priorities. Centralised models dominate when cost or control is a priority, whereas businesses seeking growth and agility often adopt federalised IT structures. Whatever the model, IT leaders should be held accountable through scorecards that measure value delivered to the business in the form of efficiency, agility, and risk levels. Scorecards should be intuitive for even the least IT-savvy board member, and they should be aligned with executives' incentives.

Questions to ask:

- What is our operating model for IT, and is it aligned with our business priorities?
- Who is accountable for delivering business value from IT—both overall and by activity?
- Are those accountable being measured using business-friendly scorecards that create the right incentives?

8. Are we comfortable with our level of IT risk?

Cybersecurity is a significant and growing IT issue. Every large company's security has been breached, and most executives have a poor understanding of the risks.

But cyberattacks are just one category of IT risk. A failure of a small software component can cost a company a lot of money in customer compensation.

IT systems can also cause business-conduct risk—for instance, if automated recommendations to cross-sell products conflict with regulatory requirements.

Companies need a comprehensive system for managing IT risk that assesses the full range of risks (for example, hacking attacks, vendor failure, and technical failure) and addresses the root causes, which include redundant technology, incorrect policies, poor processes, and insufficient oversight.

Questions to ask:

- Do we have a comprehensive understanding of the IT risks we face?
- How is our level of IT risk measured, and is it aligned with the company's overall risk appetite?
- How are we reducing our IT risk on an ongoing basis?
- Who is responsible for overseeing the level of IT risk?

9. Are we making the most of

"A failure of a small software component can cost a company a lot of money in customer compensation"

—Paul Willmott

our technology story?

IT is already on the minds of analysts, customers, regulators, and shareholders, and interest will rise as enterprises become increasingly digital. In many industries, digital is likely to become the predominant sales channel.

Companies should therefore be ready to communicate their IT strategies externally.

Questions to ask:

- What are the key messages we should communicate?
- How, when, and to whom should they be communicated? **C&L**

— This article is published with prior permission from McKinsey Quarterly.

Paul Willmott *is a director in McKinsey's London office.*

MENTOR
DINESH KAUSHIK
HEAD–IT, CAPARO INDIA

MENTEE
VIVEK BHATNAGAR
IT MANAGER, CAPARO INDIA

Right Attitude is a Must for a Mentee

Q What do you look for in a mentee/mentor?

DINESH KAUSHIK There are couple of things that I aspire my mentee to possess. First of all he should have the right attitude and be a confident person. He should be eager to take responsibilities and should have self decipline. Most importantly, he should be trust worthy. I feel all these traits are a must for my mentee. Moreover, a mentee needs to understand the objectives of the company and should always yearn to achieve those specific goals.

VIVEK BHATNAGAR A mentor should have a vision related to the IT department which should be in sync with the company's vision. He should be able to provide the right directions to the juniors so that they can grow under him and one day become leaders themselves. It is always beneficial to have a CIO in the organisation who has a vision not only for the organisation but always for the subordinates. I feel this quality is present in my mentor.

Q How do you identify and prioritise areas where you think your mentee needs to focus on for further professional development?

DINESH KAUSHIK I need to look at the background of the mentee to understand his areas of specialisation and then specify the priority areas for him. We normally have face-to-face discussions to decide what are the things a mentee should be doing in the organisation. As a CIO, I have to notice the mentee's interest areas and

then create specific goals for him which will in turn help him to grow not only professionally but also personally. I have always believed that interpersonal relationships are very important for professional development and I keep on telling this to my mentee. By imporving interpersonal skills, the mentee gains leadership traits because when one becomes a leader, he has to work in tandem with varied departments to achieve any goal for the company.

Q Do you think your mentor spends enough time with you? How do you think your mentor could contribute more towards your professional growth?

VIVEK BHATNAGAR Time is very precious and managing time is a real problem. We have to understand that a mentor-mentee relationship is not like a teacher-student relationship because here the mentee needs to understand a lot of things because the mentor trusts him to do so. I think my mentor spends enough time and if he is not there, we can communicate over the phone and get any confusion sorted out. Another important thing to know is that a CIO has to be in constant touch with the management and cannot be involved in operational work and so I am made responsible to look after the day-to-day operational tasks. The spectrum of a CIO and a IT manager is completely different and we need to respect that. A CIO has to look at the overall picture and try and make the IT department a profit centre. We as
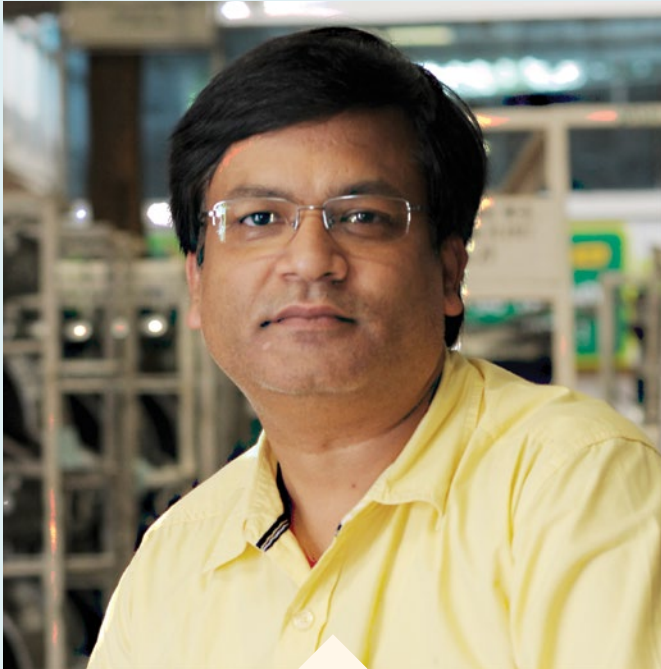
IMAGES BY SUBHOJIT PAUL

"I have always believed that interpersonal relationships are very important for professional development"

"We have to understand that a mentor-mentee relationship is not like a teacher-student relationship"

team members should assist him in achieving this goal.

Q How do you think your mentee can take on more responsibilities and take more/bigger decisions?
DINESH KAUSHIK Taking up responsibilities completely depends on the commitment of that person. I have always been target-oriented in my approach and that helps me to delegate responsibilities to my mentee. There have been numerous instances where the mentee has taken decisions on my behalf so that there is a smooth work flow in the organisation.

Q Does your mentor delegate enough tasks and responsibilities to you? How often do you take key decisions yourself? How would you like the situation to change (if at all)?
VIVEK BHATNAGAR I always believe that tasks are given according to the allocation needs of the company and a CIO delegates tasks according to the targets given to him by the management. My mentor keeps on delegating numerous tasks to me which he feels I will be able to accomplish. It is very important to delegate tasks according to the capabilities of the mentee.

Q Are there any conflicts between you and your mentee? If so, how do you resolve them? If not, what do you think is the secret of your smooth working relationship?
DINESH KAUSHIK There have been varied instances where I have had

conflicts with my mentee but we talk and sort it out. If my mentee doesn't agree with me then I have to logically explain why I am thinking in the way I am, and this solves the matter.

Q Please describe your working relationship with your mentor and how the two of you address key challenges together or resolve any conflicts of opinion?
VIVEK BHATNAGAR Our working relationship is pretty smooth and we work according to the requirements of the company. Our focus is to ensure that we leverage IT to the optimum. If there are any challenges, we try and find appropriate solutions which will help the organisation.

Q What are the two or three key things you have learned from your mentee/mentor?
DINESH KAUSHIK I like the attitude of my mentee. He takes responsibilities and is accountable. Moreover, I have faith in my mentee which is very important when it comes to delegating difficult tasks.
VIVEK BHATNAGAR I like my mentor's decision taking abilities. Another admirable quality about Dinesh is that he has the passion to take challenges. In a manufacturing company, it is not that easy when it comes to new IT deployment, but my mentor has successfully implemented many solutions in the organisation. Moreover, hard work and patience is also a very important trait which my mentor possesses.
—*As told to Atanu Kumar Das*

An Open Letter to Adventure Clubs With an Interest in Alpinism
Some organisations had a vision to do the 'Seven Summits'

I THINK many adventure clubs here have a fine tradition of moderate adventures here and abroad and have the critical mass to enable year-round activities. This is something that the Mountaineering Society has had a problem achieving. This weakness is also possibly explained by the fact that we have a very narrow focus and small membership base!

However, this narrow focus has helped us concentrate information and experience in doing what most of the active MOSS members enjoy: technical or classical style mountaineering on rock, ice and snow.

In it's 10th year now, I can look back at MOSS's(the Mountaineering Society of Singapore) achievements with satisfaction – that we focused on pushing our limits and helped shape Singapore mountaineering.

I have received feedback on not only some of the recent alpine trips made by other Singapore organisations. As tropical-based climbers in a broad-based adventure club, I think alpine mountaineering will always remain somewhat committing in terms of training, skill, experience and cost. For most of working people, it is a luxury of sorts.

Some organisations had a vision to do the 'Seven Summits', to climb all the highest seven continental summits. However, it is a goal only attainable after substantial investment and time climbing other mountains before attempting some of these objectives. All of the seven summits are extremely costly to organize and some are downright extreme in their location and commitment. Some of those climbing these peaks are also climbing for the wrong reasons: inexperienced wealthy, ill-informed (or sponsored) Walter Mittys who are often a danger to themselves.

ABOUT THE AUTHOR

David Lim, Founder, Everest Motivation Team, is a leadership and negotiation coach, best-selling author and two-time Mt Everest expedition leader. He can be reached at his blog http://theasiannegotiator.wordpress.com, or david@everestmotivation.com

The current level of experience and skill in most adventure clubs is such that I believe some of these goals can only be attained by participating in highly expensive, professionally guided expeditions. These guided expeditions advertise regularly and people here and abroad are often taken by their promises and glossy brochures. In many cases like Carstenz Pyramid, there will only be two-three days of actual climbing, making it, as one person put it, the 'world's most expensive one-day climb'. Sadly, I feel that some may feel pressurised into putting all their resources in these interesting objectives without focusing on the key issue that a good mountaineering foundation will pay its dividends in the future through self-organised expeditions. Such trips will be eminently more satisfying in not only achievement and learning, they will be significantly cheaper to organise. Such confidence can only come about through training on successively harder, smaller peaks such as those in the Alps. Failure will be commonplace. But eventually, the experience gained will be invaluable in the higher ranges. I see a two-week summer alpine climbing trip to a region like the Cascades, Alps etc. to be more beneficial to many budding alpinists than a trip to say Island Peak in Nepal. The latter will eat up four-weeks of leave and involve only two days of actual climbing. A two-week alpine trip may see one bagging experience through climbing up to five peaks over 10 solid days of climbing. Much better value. Sadly, in Singapore the former option seems to carry more attraction and glamour than the latter. We seem to be in a society which is in a hurry to succeed at anything.

A few years ago, a group from Singapore did make

> "A two-week alpine trip may see one bagging experience through climbing up to five peaks over 10 solid days of climbing. Much better value"

IMAGE BY PHOTOS.COM

a failed attempt on Island Peak, a popular, straightforward Nepal peak. A member of that group made an unsolicited request for advice. It appeared they 'had' to climb a 6000-metre peak to win the necessary sponsorship for their trip. Of the ten, only one had had a short three-day climbing course. And they were oblivious that their intended February ascent would be in the winter! I advised them that the money would be better spent on a technical climbing course for the group. After all, peaks would also be climbed in the course of this trip. I also offered them a weekend alpine skills course which would have given them some life-saving skills. The refused all of this, preferring to be hauled up Island Peak by fit, if technically inept sherpas.

The cheek of it was that their leader was publicly quoted as saying "safety is of the paramount importance!"

This, sadly is not an isolated case. Ultimately, those in adventure clubs who intend to participate in alpine-climbing activities must ask themselves what their goals are and whether they are financially and socially committed in going for them. Success on the mountains is hard to come by and I feel too many aspiring climbers here are enamored by the thought of success on the big peaks rather than the necessary and hard apprenticeship that has to precede such success. I think many people can enjoy this form of climbing at a far less committing level, and enjoyment, after all, is what makes us stay in

this sport. In the past, some of my strong views have not gone down well with members of the climbing community but I hope that recent events and expeditions illustrate that the gaining of experience should take precedence over ambition. Generally, myself included, we are resistant to taking advice from people if this advice is in conflict with our desires! However, commonsense (all too lacking) must prevail. Members of MOSS(Ed Note: Mountaineering Society of Singapore) with the right experience have been sharing it with interested parties. Some have started out on the right foot, gaining experience through alpine-training courses and then striking out on their own to apply these skills in the mountains. Unfortunately, some of those from other organizations who have approached us for advice on certain over-ambitious climbing objectives have refused to accept the advice given and have met with failure. CLIMB 2000, an exciting mountaineering project, will be launched next year. It will comprise a grassroots educational component which will benefit many budding alpinists, a Foundation programme to fund and train climbers with little alpine experience and an Excellence program for the top papayas of Singapore's climbing community. **C&L**

DAVID LIM IS A LEADERSHIP AND NEGOTIATION COACH AND CAN BE FOUND ON HIS BLOG http:// theasiannegotiator.wordpress.com, OR subscribe to his free e-newsletter at david@everestmotivation.com

"If you ever find yourself in a tight, unanimous group, you must speak your mind, even if the team does not like it" —ROLF DOBELLI

The Art of Thinking Clearly

Eliminating all errors is the key to success
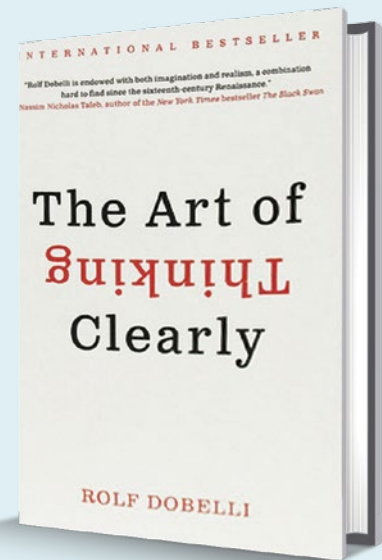
THE POPE asked Michelangelo: " Tell me the secret of your genius. How have you created the statue of David, the masterpiece of all master pieces? Michelangelo's answer: Its simple I removed everything that is not David."

In his book, Rolf Dobelli (born 1966) a Swiss novelist, writer and entrepreneur, highlights that people do not know what makes them successful. Equally it is hard to pin point what make them happy. But everyone knows what makes them feel bad and what kills success or destroys happiness. The realisation highlights the fundamental of thought process and decision making where in Negative Knowledge (what not to do) is more potent than Positive Knowledge (what to do).

The book, spreading in 99 small chapters, shrewdly tells us to to adopt Michelangelo's method to think clearly, which means do not focus on David, instead focus on everything that is not David. The Greeks, Romans and Medival thinkers gave it a term; Via Negativa. Practically speaking Via Negativa means elimi-nate all errors, things which destroy happiness, kill success to have a clear and better thinking.

Even Warren Buffett, the investor billionaire, has accepted the importance of Via Negativa thought process in building his successful business empire. While writing about himself and his partner Charlie Munger, Buffett writes: Charlie and I have not learned how to solve difficult business problems. What we have learned is to avoid them.

One of the best things about the book is that the author has experimented some of the suggestions on himself before penning it down in the book. In one of the chapters — Why you should not read the news — the author says that news is to the mind what sugar is to the body: appetising, easy to digest, but highly destructive in the long run. Rolf Dobelli, as an experiment stopped reading and listening to news for three years. He says the first few weeks were difficult. But after a while he had a completely new outlook. He had clear thoughts, valuable insights and better decision making ability. Even, despite not reading or listening to news, he

ABOUT THE AUTHOR

Rolf Dobelli is a Swiss novelist, writer and entrepreneur. He is the founder of zurich. minds.
He was born in 1966 in Lucerne, Switzerland.
He co-founded getAbstract, a publisher of book summaries and article abstracts.

remained well informed about the development happening around through his social circles, which acted as a news filter. He suggests readers to read long background articles and books to understand the world in a better way. The book originated from the notes and personal anecdotes, which the author has taken from himself to avoid frivolous gambles with the wealth he has created while writing. Later it turned into newspaper columns and then finally a book.

Rolf Dobelli says that whatever he has discussed in the book is not everything. In one of the discusions in the book, the author says that majority of errors are related to each other.

Even the author is not a social scientist, but a entrepreneur and novelist. But the books is an interesting read. It certainly does not guarantee success and happiness. But it would be a great help for the people who are open to experiment to improve their thought process and avoid some of the errors while climbing the ladder of success. **C&L**

—By Akhilesh Shukla

IMAGE BY PHOTOS.COM

Hacking Back is a Bad Idea

The idea of "hack-back" is best left to 007 and his army of hacker-geeks   **By Rafal Los**

The topic has been kicked around so much that there are now government commissions issuing reports and senators are chiming in. Private industry and corporations alike are talking about "hack-back." It's no secret I believe that "hack-back" is a bad idea, for many reasons. The conversation on Twitter yielded little favor for "hack-back" in my circle of friends/followers, as Wireheadlance questioned the long-term benefits, and Tadd Axon even had trouble with any provable short-term benefits.

The short version is this: I believe if you look at the enterprise space, "hack-back" is applicable as more than just a fancy neat idea to about .05 percent of organisations. There are a few reasons for this, including resources, attribution, and others I outline in an article I published last week.

As I was thinking about how best to explain why "hack-back" is a bad idea to the executives I talk to, an analogy from my childhood comes to mind. As a kid I went to one of those average schools in suburbia. Kids followed the playground rule of "If you hit me, I'll hit you back until someone wins." The problem with this approach is that it almost always ended with either the recess bell calling us back from the playground or, more likely, a teacher breaking up a massive brawl.

You see, when someone hits you and the only way you perceive to stop them is to hit back, you have to make sure you are in a position where your hit-back will be the end of the incident. In the primary school where I went this was rarely the case. I bet you're thinking that Information Security professionals and enterprises don't behave like primary schoolers — right? If that's the case you've clearly not been around the industry long!

Anyway, when Kid A smacks another, Kid B hits back, and then they start beating on each other and a tap can quickly escalate to punches and the brawl starts to pull in friends, bystanders and other kids who had no interest in engaging in a fight. What started out as one quiet kid getting lightly picked on by a bigger kid can quickly escalate into a big-time brawl. I witnessed this, and even had the displeasure of being at the center of this type of thing in primary school many times, I can tell you it's a fact.

So now let's move onto how "hack-back" is different in the enterprise than on a primary school playground. There are clear differences, but I don't think they are great enough to make one case inapplicable to the other.

First off, in cyberspace attribution is a little harder. On the playground you can see the person who hit you ... well, almost always. Sometimes you're turned around, standing

Now in cyberspace we can track IP addresses and TTPs from specific threat actors, which smart analysts and researchers tell us is a viable way to perform attribution

in line waiting to get into school, and from behind you somewhere someone flicks the back of your ear. It hurts. So you turn around to hit back except that you have no idea who hit you. None of the other kids want to get hit, so they won't easily give up the person who did the flicking. You're left deducing the antagonist on your own, and odds are good you're going to retaliate against the wrong person. It happens all the time!

Now in cyberspace we can track IP addresses and TTPs from specific threat actors, which smart analysts and researchers tell us is a viable way to perform attribution. I agree with them, largely, but there's a fault there. An IP address belonging to China SQL injecting your enterprise applications is hardly a smoking gun that Chinese APTs are after you. Attackers have been using others' modus operandi to mask their identities for as long as spy games have been played. Attackers have been known to use compromised machines and proxies in hostile countries for as long as I can remember caring — to "bounce through" to attack you. Heck, many of the attacks that appear to be originating from nation-states that we suspect are hacking us may very well be coming from a hacker at the coffee house next door to your office, using multiple proxies to mask their true origin. This is just good OpSec, and attackers use this method all the time, let's not kid ourselves.

The next big problem you have if you're turning around to retaliate after your ear

33%
OF OFFICE SOFTWARE USERS WILL BE USING CLOUD BY 2017

has just been set afire by a strong flick from behind is the size/strength of the kid who hit you. What if you're an average-sized kid and the person that just hit you is a big bully? You hit him or her back and then what? A punch to the face, or an atomic wedgie that's what. Now you've incurred the wrath of the bully, whereas the flick was just a playful thing without intent to really hurt. This is how things escalate. In the enterprise it's the same thing. If your forensics tell you that you're being attacked from a specific origin, going and attacking them back may actually make things much worse.

Let's say you find an attacker originating from within the Russian Federation IP space. You locate, identify and strike back at the system being used to attack you — completely disabling it. Now maybe that system is no big deal, or maybe you've now taken down a critical Russian government server and caused a diplomatic incident. I know this is an extreme case, but the point is no less valid.

Remember folks, the saying "an eye for an eye" leaves the whole world blind. The idea of "hack-back" is best left to 007 and his army of hacker-geeks, because in real life unless you're part of that .05 percent, you're likely to make things worse for yourself. Maybe this is just one of those things enterprises leave up to the professionals if they find themselves in dire straits with no other options. C&L

— This article is printed with prior permission from www.infosecisland.com. For more features and opinions on information security and risk management, please refer to Infosec Island.

Over-Sharing Riskier than Govt Snooping

The fact is that people in this age of the Internet freely share huge amounts of personal info on a daily basis, and doing so puts them at risk By Anthony M. Freed

There has been an uproar over disclosures regarding the rather ambitious programme known as PRISM and the harvesting of metadata from mobile phone calls, both programmes administered by the NSA which are designed to gain access to what we would like to think is private information. While the widespread rage over the government engaging in the systematic collection and analysis of data about law abiding citizens is more than understandable, the fact is that people in this age of the Internet freely share huge amounts of personal information on a daily basis, and doing so puts them at risk.

We freely share details of our lives, our travels, information about our children, our extended family, about our business, our employers, our Web browsing and shopping habits, our medical condition – all data that falls under the definition of Personally Identifiable Information (PII). This information, when aggregated in Big Data systems, can reveal very personal details about nearly every aspect of our lives. And it's not just the government we should be worried about in the application of this information, it's also big business marketing machines and even worse – attackers who seek to exploit these open sources of intelligence for their own gain.

The NIST's Special Publication 800-122 defines PII as "any information about an individual... that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name..." but it encompasses far more. "The definition of PII that most people understand is really far too narrow. PII is really any piece of information that can be used to confidently link data back to a human," said Andrew Storms (@st0rmz), director of security operations for Tripwire.

His colleague Lamar Bailey (@btle310), director of security research and development, agrees. "PII is not just credit card, Social Security numbers, and bank accounts. It's literally any information that can used to impersonate you or gain your trust online and offline."

PII is routinely collected every single day of our digital lives – through tracking cookies when we visit websites, keywords in emails we send, through purchases made with credit or debit cards, when we scan parking or public transportation passes, and more –

all of it together producing a portrait of our very selves.

"Here's an example that involves department store and grocery store rewards cards," Storms points out. "Last year, Target got in trouble for using consumer purchase data to identify a pregnant teenin before her parents knew."

This type of data is quite valuable to the businesses we patronise, and it is also often sold to other commercial interests. While we might expect the businesses we frequent to use this data in an attempt to tailor our shopping experience, there are much more nefarious elements who find this data valuable as well, which is why it is so often the target of criminal cyber attacks.

Aside from the vast amounts of data stored by organisations that can be exfiltrated by hackers, there is even greater amounts of personal information readily available that we ourselves produce and distribute through social media platforms – information that can be used against us. "Many people don't think like attackers, and trustingly add their information to online sites like high school yearbooks, birthday reminders, and genealogy or family tree sites that are prevalent on social media," said Tripwire's CTO Dwayne Melancon (@ThatDwayne).

"For an attacker that is targeting you or attempting to steal your identity, these sources are a gold mine."

And it's not just personal details we are broadcasting through social media, we may also be providing clues to attackers that can be utilised in brute force and dictionary attacks designed to gain access to our accounts. "Attackers can also mine a wide range of social sources to find out the answers to your 'secret questions' for identity validation – where you went to school, mother's maiden name, previous addresses, and things like that," Melancon pointed out.

Storms agrees, pointing out that "one of the most significant attacker innovations recently has been the ability to tie multiple smaller bits of information together as part of a cohesive attack strategy. Social media and networking sites are treasure troves of data that users unknowingly give away every day."

It is not only our personal assets and accounts that are being targeted through data mining of social networks, it is also our businesses or our employers who may be the real target of such operations.

IMAGE BY PHOTOS.COM

The bottomline is that every piece of electronic data about you is being captured and analysed

"Attackers are not just looking for PII, they also look for ways to get data from others that can be used against you," Melancon said. "For example, people who want to gain information about company executives may mine Facebook looking for informative posts from the executives' family and friends."
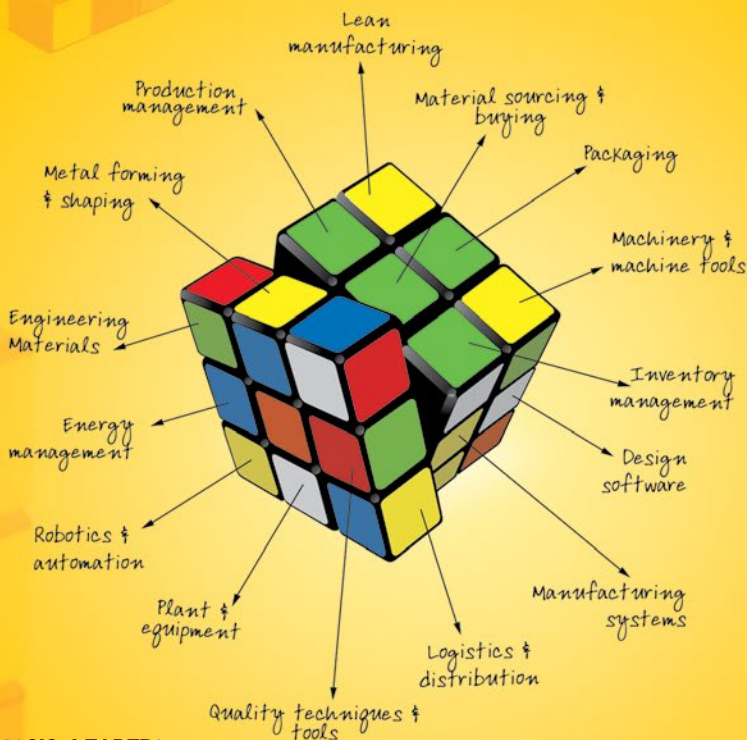
So this is the age we live in. No, there is not a lot we can do about big business and big government utilising Big Data stores – that issue lands squarely with our elected officials who need to enact strong data collection and use laws.

But, there are some precautions we can take in an effort to not over-share personal information. Just how much damage we have already done to our own privacy and security remains to be seen.

"The bottomline is that every piece of electronic data about you is being captured and analysed," Storms said. "With enough data and compute cycles, just about anyone can be identified and 'hacked' without the traditional PII data points." C&L

— This article is printed with prior permission from www.infosecisland.com. For more features and opinions on information security and risk management, please refer to Infosec Island.

CSO FORUM

Security For Growth And Governance

THE MID-YEAR CSO SUMMIT

With the aim to arm CSOs with better cyber security tactics in dealing with state sponsored attacks, detecting breaches and creating a response mechanism, 9.9 Media organised The Mid-year CSO Summit **By Debashis Sarkar**
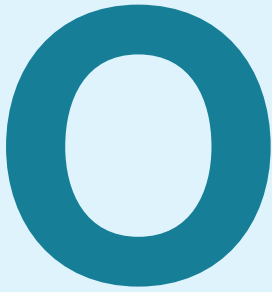
O

peration Ababil. The $45 million global ATM heist. The DDoS attack on Spamhaus. State sponsored attacks. When it comes to securing crucial business data, it has always seemed less than what meets the eye. The current Indian IT Act seems toothless in fighting cyber crime. At a time when the government is slowly waking up to the crisis, CSO Forum hosted the first Mid-year CSO Summit to unite prominent CSOs pan-India to share their experiences and wisdom. The two-day event was attended by more than 55 CSOs.

CSO Forum calendar till last year included The Annual CSO Summit and three Regional (CSO Think Tank) Summits. To increase the frequency of engaging the community, 9.9 Media organised The Mid-year CSO Summit. The two-day event was scheduled from 21-22 June, at The Trident Gurgaon. The event aimed at arming CSOs with better cyber security tactics in dealing with state sponsored attacks, protecting web applications, detecting breaches and creating a response mechanism.

The first day of the summit had an interesting and relevant session on "UID- Implications for CISOs". Yogesh Bhatia, Practice Lead – Secure Development Lifecycle Service, Aujas walked through different aspects of UID.

"Aadhaar is not a typical ID card. UID uses biometric de-duplication. Aadhaar doesn't utilize face photo to identify. For every new enrollment we de-duplicate it against 360 million Aadhaar IDs issued. Every finger print goes to three independent biometric

vendor validation. Finally, Aadhaar is an irrevocable identity," said Bhatia.

Security experts have regularly pointed out that most organisations do not get to know about any breaches till a third party tells them. How can then one expect them to respond?

"Nobody expects to be breached and yet we do face such instances," said Vivek R Chudgar, Director, FireEye Labs (APJ).

In a session on Detecting Breaches and Creating a Response Mechanism, Dr. Krishna Sastry, Cyber Forensics Scientist and Former Govt Examiner said, "Low value assets are the first target. Everything is more focused on indirect attacks and organisations have to strike a balance between business and technical requirement for IT security."

"PSU employees violate security policy. It is very common to see PSU employees connecting pen drives after 7 pm on Saturdays. It is also very important to note that if you shutdown the system, you will lose evidence," added Sastry.

Dr. Gulshan Rai, Director General, CERT-In, Government of India addressing CSOs on the second day of the summit

More than 55 CSO participated in the two day event

KS Narayanan, CISO, ING Vysya Bank opined, "A good malware strategy is crucial."

The summit had a panel discussion on the important subject of "Evaluating the value of real security" moderated by Shivangi Nadkarni, Co-founder and CEO, Arrka Consulting Services. The session included panelist such as Subhash Subramanian, CISO, ICICI Bank; Parag Deodhar, Chief Risk Officer, CISO and Vice President , Bharti Axa and Akash Mainra, Manager - Enterprise Sales, Blackberry Enterprise Products.

CISOs constantly have to strike a balance between a portfolio of ideal security programmes and the realities of a budget. While this is certainly a challenge for the CISO, what is the view from 'the other side'?

"We cannot ignore BYOD anymore," said Mainra. "Pressure on IT security budget still remains," pointed Nadkarni.

"I see a change in the way IT security is looked at. There is more interest in investing in threat detection," said Subramanian.

"CFO still looks at numbers. ROI remain in the top priority list. However, value addition helps us to get budgets," said Deodhar.

The session on "Dealing with state sponsored attacks - should CISOs be worried?" witnessed an interesting discussion among Felix Mohan, CISO, Airtel; Subramanian V, CISO, IDBI Bank and Vinod Vasudevan, COO & Co-Founder, Paladion Networks.

State sponsored attacks now targeting businesses, "Criminals are doing a huge amount of research. There is a huge cyber criminal network globally. Criminals using military-grade exploits. Inter-criminal gang competition betters their malware arsenal. I think we should be worried," said Mohan.

Vinod Vasudevan, COO & Co-Founder,

Security experts have regularly pointed out that most organisations do not get to know about any breaches till a third party tells them

Paladion Networks opined, "Nation state attack can impact enterprises big time. Indian government should be worried about state sponsored attack. Critical national infrastructure cloud face mass attacks. However, Indian enterprises can feel safe for the moment."

"We need to respond quicky and engage with experts to tackle the issue," said Subramanian V, CISO, IDBI Bank.

So, is there a need for support from the government? This question elicited different responses from the CSOs.

While Mohan said, "Government requires private sector support in dealing with cyber security and not us." Vasudevan felt, "Government should fund private sector to fight cyber crime."

Meanwhile Subramanian said, "There is a need to start building security from ground up. Public awareness is required."

Discussing new trends in DDoS and mitigation strategies, Jeff Buhl, Vice President & GM – Asia Pacific, Arbor Networks gave valuable insights into security breaches.

"Over 28 million open DNS servers are

Vikas Gupta, Founder & Director, 9.9 Mediaworx setting the agenda for the two day event while welcoming the participants

present globally. Attacks targeting port 53 has increased dramatically from 2 per cent to 7 per cent," he said.

In a discussion on protecting web application, Dhananjay Rokde, Global Head - Information Security, Cox & Kings; Subrahmanya Boda Gupta, GM - IT Security & Governance (CISO), GMR Group; Jonathan Andresen, Director, Product Marketing, Asia, Bluecoat and Pawan Kinger, Vulnerability Research Manager, Trend Micro participated.

Gupta pointed, "Put any number of encryption to secure your application. If you don't have internal strength in it, there will be threats." Andresen felt, "Too many layers of security slow down web apps."

"CISO are busy building walls to protect web applications. But the problem is they don't know from what they are protecting their apps,"added Rokde.

"Injection/cross-site scripting can be protected outside of the application. Web application vulnerabilities are the first entry point to send infection on web servers," said Kinger.

CCM or Continuous Controls Monitoring is becoming an increasing popular tool to provide a snapshot of the state of automated and manual controls for an organisation. In this session on CCM, Pankaj Agrawal, Head of IT Governance and CISO, Aircel highlighted, "Companies lose about 0.5% in duplicate payments, 4.6% of invoices contain errors and 44% of companies pay without original invoices. This leads to economic crisis."

"CCM solution sits above IT systems and provides 100% secure transactions. Also, there is no need to audit people if someone has an automated CCM," added Agrawal.

The unit of security is gradually moving on from data to the individual and in such a scenario identity and its federation can provide much needed intelligence and levers for governance. So, how are organisation looking at Identity Access Management?

"Next gen firewall: dont get into marketing hype, you may already have what you need in your established security infrastructure," said Vishak Raman, Senior Regional Director, Fortinet.

"We give roll-base access to apps. We take control while providing IDs," said Satish Warrier, CISO, Godrej Industries. "We should make ID management smart. At Godrej, we disable IDs inactive for 60 days."

Subhash Subramanium, CISO, ICICI Bank said, "We have 2000 priviledged IDs and 60,000 outsourced IDs. Although we do review exercise every three months, size of access management has been creating problems.

On the second and final day, The Mid-year CSO Summit hosted a workshop on cyber forensics and cyber law- creating an incidence response mechanism.

Dr. Gulshan Rai, Director General, CERT-In, Government of India addressed the state of cyber security in India by saying, "The incidences that we witness today are far more complex. It's time to have a close collaboration between the industry and government to achieve in this domain. India due to its growing economic influence worldwide, has gained attention from cyber criminals. This is the time to come and think together as to what is best for the country. The scenario of cyber security in India needs to be improved significantly." **C&L**

More than 55 CSOs participated in the two day event

KS Narayanan, CISO, ING Vysya Bank opined, "A good malware strategy is crucial."

The summit had a panel discussion on the important subject of "Evaluating the value of real security" moderated by Shivangi Nadkarni, Co-founder and CEO, Arrka Consulting Services. The session included panelist such as Subhash Subramanian, CISO, ICICI Bank; Parag Deodhar, Chief Risk Officer, CISO and Vice President , Bharti Axa and Akash Mainra, Manager - Enterprise Sales, Blackberry Enterprise Products.

CISOs constantly have to strike a balance between a portfolio of ideal security programmes and the realities of a budget. While this is certainly a challenge for the CISO, what is the view from 'the other side'?

"We cannot ignore BYOD anymore," said Mainra. "Pressure on IT security budget still remains," pointed Nadkarni.

"I see a change in the way IT security is looked at. There is more interest in investing in threat detection," said Subramanian.

"CFO still looks at numbers. ROI remain in the top priority list. However, value addition helps us to get budgets," said Deodhar.

The session on "Dealing with state sponsored attacks - should CISOs be worried?" witnessed an interesting discussion among Felix Mohan, CISO, Airtel; Subramanian V, CISO, IDBI Bank and Vinod Vasudevan, COO & Co-Founder, Paladion Networks.

State sponsored attacks now targeting businesses, "Criminals are doing a huge amount of research. There is a huge cyber criminal network globally. Criminals using military-grade exploits. Inter-criminal gang competition betters their malware arsenal. I think we should be worried," said Mohan.

Vinod Vasudevan, COO & Co-Founder,

Security experts have regularly pointed out that most organisations do not get to know about any breaches till a third party tells them

Paladion Networks opined, "Nation state attack can impact enterprises big time. Indian government should be worried about state sponsored attack. Critical national infrastructure cloud face mass attacks. However, Indian enterprises can feel safe for the moment."

"We need to respond quicky and engage with experts to tackle the issue," said Subramanian V, CISO, IDBI Bank.

So, is there a need for support from the government? This question elicited different responses from the CSOs.

While Mohan said, "Government requires private sector support in dealing with cyber security and not us." Vasudevan felt, "Government should fund private sector to fight cyber crime."

Meanwhile Subramanian said, "There is a need to start building security from ground up. Public awareness is required."

Discussing new trends in DDoS and mitigation strategies, Jeff Buhl, Vice President & GM – Asia Pacific, Arbor Networks gave valuable insights into security breaches.

"Over 28 million open DNS servers are

present globally. Attacks targeting port 53 has increased dramatically from 2 per cent to 7 per cent," he said.

In a discussion on protecting web application, Dhananjay Rokde,Global Head - Information Security, Cox & Kings; Subrahmanya Boda Gupta, GM - IT Security & Governance (CISO), GMR Group; Jonathan Andresen, Director, Product Marketing, Asia, Bluecoat and Pawan Kinger, Vulnerability Research Manager, Trend Micro participated.

Gupta pointed, "Put any number of encryption to secure your application. If you don't have internal strength in it, there will be threats." Andresen felt, "Too many layers of security slow down web apps."

"CISO are busy building walls to protect web applications. But the problem is they don't know from what they are protecting their apps,"added Rokde.

"Injection/cross-site scripting can be protected outside of the application. Web application vulnerabilities are the first entry point to send infection on web servers," said Kinger.

CCM or Continuous Controls Monitoring is becoming an increasing popular tool to provide a snapshot of the state of automated and manual controls for an organisation. In this session on CCM, Pankaj Agrawal, Head of IT Governance and CISO, Aircel highlighted, "Companies lose about 0.5% in duplicate payments, 4.6% of invoices contain errors and 44% of companies pay without original invoices. This leads to economic crisis."

"CCM solution sits above IT systems and provides 100% secure transactions. Also, there is no need to audit people if someone has an automated CCM," added Agrawal.

The unit of security is gradually moving on from data to the individual and in such a scenario identity and its federation can provide much needed intelligence and levers for governance. So, how are organisation looking at Identity Access Management?

"Next gen firewall: dont get into marketing hype, you may already have what you need in your established security infrastructure," said Vishak Raman, Senior Regional Director, Fortinet.

"We give roll-base access to apps. We take control while providing IDs," said Satish Warrier, CISO, Godrej Industries. "We should make ID management smart. At Godrej, we disable IDs inactive for 60 days."

Subhash Subramanium, CISO, ICICI Bank said, "We have 2000

Vikas Gupta, Founder & Director, 9.9 Mediaworx setting the agenda for the two day event while welcoming the participants

priviledged IDs and 60,000 outsourced IDs. Although we do review exercise every three months, size of access management has been creating problems.

On the second and final day, The Mid-year CSO Summit hosted a workshop on cyber forensics and cyber law- creating an incidence response mechanism.
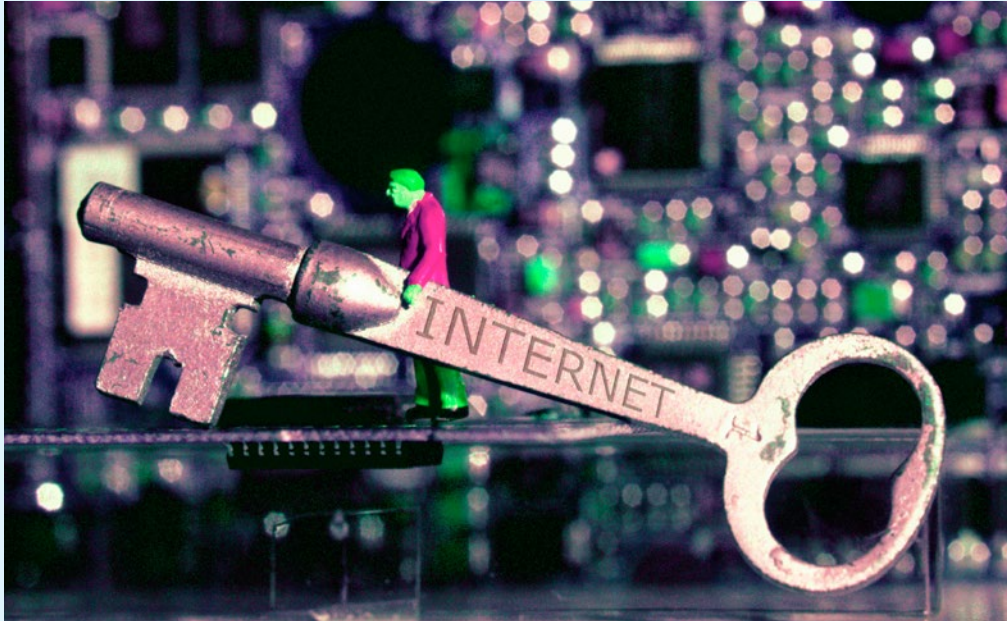
Dr. Gulshan Rai, Director General, CERT-In, Government of India addressed the state of cyber security in India by saying, "The incidences that we witness today are far more complex. It's time to have a close collaboration between the industry and government to achieve in this domain. India due to its growing economic influence worldwide, has gained attention from cyber criminals. This is the time to come and think together as to what is best for the country. The scenario of cyber security in India needs to be improved significantly." C&L

IN-SHORT

Cyber Security Spending To Hit $46 Billion Globally

estimates that cyber security spending for critical infrastructure will hit $46 billion globally by the end of 2013. Increased spending over the next five years will be driven by a growing number of policies and procedures in education, training, research and development, awareness programs, standardisation work, and cooperative frameworks among other projects. The digitisation of critical infrastructures has provided substantial benefits in terms of socio-economic developments improved productivity, better connectivity, greater efficiencies. Yet some of these attributes also carry significant risks. Always-on Internet connectivity has ushered in a new cyber-age where the stakes are higher. Disruption and destruction through malicious online activities are the new reality: cyber-espionage, cyber-crime, and cyber-terrorism. The cyber protection of critical infrastructure has become the most immediate primary concern for nation states. The public revelation of wide-spread state-sponsored cyber-espionage presages an era of information and cyber warfare on a global scale between countries, political groups, hacktivists, organised crime syndicates, and civilian society " in short, to anyone with access to an Internet-connected device.

The focus on cyber security is becoming imperative. While some industries have had highly advanced cyber-defense and security mechanisms in place for some time (i.e. the financial sector), others are severely lacking and only just starting to implement measures (i.e. energy, healthcare). This Market Data on 'Critical Infrastructure Security' breaks down spending for eight verticals: Defense, Energy, Financial, Healthcare, ICT, Public Security, Transport, and Water and Waste Management.

Data Briefing

10.9% decline in PC shipment s in the second quarter of 2013

ITTIA Brings Big Data On Mobile

ITTIA announces the big data capabilities of ITTIA DB SQL, a modern database for smart embedded systems with limited local resources. With this unique technology, a large data set can be distributed across a wide array of devices, with the potential to store millions of rows per device. Applications can then run queries on individual devices, or pool data together in a back-end system for data warehousing and data mining. In this way, developers benefit from highly reliable embedded database software with a strong track record in mission-critical systems.In recent market evolutions, developers of applications for embedded systems – including medical devices, industrial automation, automotive software, and mobile tablets – often encounter serious data management challenges in which a large amount of data is collected and accumulated at different locations. Typical queries required by end users of these systems are not easily met.

IN-PERSON

Diwakar Dayal
Lead - Security, Borderless Networks
Sales, Cisco India & SAARC

"Security is a Boardroom Issue"

In an interview with Akhilesh Shukla, Diwakar Dayal, Lead - Security, Borderless Networks Sales, Cisco India & SAARC discusses DSCI and Cisco security report

Q **What steps does a CISOs need to take to re-assess his security ecosystem and evaluate capabilities of next generation security?**
With security gradually becoming a boardroom issue, the CISOs role has evolved dramatically over the last couple of years. CISOs need to undertake a series of calculated steps to reassess their security ecosystem and evaluate capabilities of next generation security including. They need to make an assessment to identify assets, and uncover any vulnerabilities which may pose as a possible risk. CISOs should evaluate if the existing solution can 'Defend, Discover and Remediate' advanced security risks.

Q **Your report says existing solutions may not withstand challenges of BYOD, mobility and virtualization. In that**

case, what is the way forward?
Cisco and DSCI's report indicates that while 66 percent of security leaders in India encourage employees to bring their own device to work, 56 percent also believe that current solutions are ineffective in managing the security of mobile, BYOD, and virtualization. So, the way forward is to adopt a security framework that is dynamic, integrated and pervasive. Organisations should invest in deploying next gen security solutions that offer an allencompassing, defense-in-depth model which has multiple countermeasures embedded in every aspect of the user connecting to the network & accessing the applications. They should look at deploying a 'holistic security policy' so that data access controls can be applied securely to devices on wired, wireless and even remote LAN locations

Q **Despite having sophisticated security systems in place we often see security breaches. Please comment.**
Securing and managing the distributed and agile networks has become a challenging undertaking, and cybercriminals are targeting mission critical data with sophisticated attacks. Additionally, traditional security, which relies on layering of products and the use of multiple filters, is not enough to defend against the latest generation of cyber attackers who are dynamic, have global targets, and use multiple vectors to propagate.

Q **Should organisations put a blanket ban on social networking websites?**
With increased adoption of Web2.0 technologies including social media, wikis and even video, CTOs are under immense pressure to be able to deliver a seamless and robust network experience to users. This is to be managed while simultaneously handling the growing issues around technology complexities, security and compliance. Implementing a blanket ban on the use of social networking websites in the workspace will not prove fruitful since the use of social media enables enhanced collaboration and productivity. **C&L**

Shifting from IPV4 to IPV6

In a conversation with Atanu Kumar Das, Mahesh Gupta, Geo-Lead, BN Sales, Cisco India & SAARC, talks about the challenges and advantages of migrating from IPV4 to IPV6

What is the need for shifting to IPV6?

The evolution of the internet has taken place at an exponential pace and although India is still grappling with bandwidth issues, there's a global barrier that needs to be overcome - the shift to IPV6. IPV6 is an obvious extension of what will eventually be critical for mass connectivity. While the term has been predominantly discussed in technology circles, it's implications for organisations and the general user community is relatively unexplained.

The exhaustion of IPV4 addresses had a major impact on the growth of the Internet, Internet service providers (ISP) and Internet presence (websites, e-commerce, email). So, the move to IPV6 (340 trillion, trillion, trillion unique IP addresses) is a viable option for the ecosystem at large.

From an enterprise perspective, the shift from IPV4 to IPV6 will be instrumental in connecting billions of people, devices and even objects to interface directly with each other or through the internet. As early adopters of IPV6, organisations will also have a chance to ensure that customers derive maximum value from their business proposition and are able to do so, on multiple devices as well as maintain business continuity.

India has already taken significant strides towards the mainstream deployment of IPV6 with the Department of Telecom (DOT) unraveling the 'National IPV6 Deployment Roadmap Version II'.

This mandates that starting January 1, 2014 all internet connections provided to business organisations should support the new version of internet addresses based on IPV6. It also states that government organisations should prepare a detailed transition plan for complete migration to IPV6 by December 2017.

How is Cisco helping enterprises in shifting to IPV6?

Cisco is a leader in the networking domain and one of the key drivers behind the IPv6 revolution. As a pioneer of IPv6 technology since 1996, Cisco is an established leader in advising organisations in their journey towards IPv6 planning and migration. IPv6 expands the number of network address bits from 32 bits (in IPv4) to 128 bits, which pro-

vides more than enough globally unique IP addresses for every networked device on the planet. However, it's not just about addressing. It's about business continuity and innovation. The unlimited address space provided by IPv6 will allows us to deliver more and newer applications and services with reliability, improved user experience and increased security.

These might include, multiple internet-enabled mobile devices for every person on

" India has already taken significant strides towards the mainstream deployment of IPV6"

the planet, billions of embedded sensors using technologies such as RFID, IEEE 802.15.4, and personal area networks, home and industrial appliances, smart grids. Organisations which choose to react to address exhaustion will find their customer base shrinking. It will be more difficult to innovate and more resources will be needed to sustain IPv4 investments. It's best to be proactive.

Cisco can help enterprises to develop a strategy to make the move to IPV6 with

three general approaches, preserve your existing IPV4 investment, prepare your organisation for growth and prosper by expanding innovation and productivity. Use Cisco service to successfully adopt IPV6. Some of our services are IPV6 discovery service to explore benefits for your IT infrastructure, IPV6 assessment service to determine necessary network changes and anticipate challenges, IPV6 planning and design service to create designs and a smooth transition strategy, IPV6 implementation service to validate network readiness and offer consulting and finally network optimisation service to help you absorb, manage, and scale IPV6 in your environment.

What are the challenges in implementing IPV6?

OIPV6 is much more powerful than IPV4, so enterprises must do proper planning before migrating to IPV6. There can be security issues and so organisations should take a holistic view. We at Cisco are working towards providing the best network security for the enterprises. Information theft can result from router impersonation (man-in-the-middle attacks), address theft, address spoofing, and remote address resolution cache exhaustion (denial of service attacks). These security breaches can come from malicious or misconfigured users, and can severely disrupt Layer 2 domains and networks in general.

The Cisco IPV6 First Hop Security (FHS) solution protects networks by mitigating these types of attacks and misconfigurations errors. It addresses IPV6 link operations vulnerabilities, as well as scalability issues in large Layer2 domains.

You gain a strong defense against attack vectors and widely available tools that exploit vulnerabilities. We at Cisco, realised the problem of security 10 years back and since then we have been working hard on this domain.

Presently, we are working with the government of India to help them train the employees in proper manner so that they can migrate from IPV4 to IPV6 in a smooth manner. We realise the importance of being a strategic partner with the government, and we are working very closely with the DOT on different aspects of deployment of IPV6. C&L

PHOTO BY PHOTOS.COM

What is Enough Security?

Enough security is not the same thing as absolute security   **By Rafal Los**

How to strike a balance between increasing security demands and similarly increasing costs of security? What --- not how much --- is enough security in the contemporary business environment in which virtual and physical worlds are inseparable? Finding answers to these questions is not an easy task.

With regard to cyber security, demands for both enhanced cooperation between private businesses and government agencies and resources allocated to address the issue are increasing. Cyber security is important because many other forms of security (e.g. national, economic, and environmental) and activity (e.g. commerce, energy supply, and transport) depend on it.

The majority of most nations' critical infrastructure is in the hands of private entities and therefore, companies are pressured to pay highlighted attention to security. Simultaneously, as for example in the United States where the implementation of the President's Executive Order tries to improve the dialogue between the private sector and the government, the responsibility to determine what is enough security is pushed onto the shoulders of companies and trade associations. They ought to know best the requirements of their own industry. The problem is that many companies do not know how to evaluate the needed security levels.

Enough security is not the same thing as absolute security. Absolute security does not exist. Thus, striving for an illusion hardly supports anyone's core business. The entwinement of virtual and physical worlds merely highlights the need to both resist and absorb security breaches as they do inevitably occur. A company needs to decide how many and what kind of breaches it will or is able to resist, accept, mitigate, and counteract. Exposure to risk varies accordingly. The more means the company uses to enhance security, the more costs it generates. Hence what one wants to do is to get the decisions concerning costly investments right.

Security involves emotions, beliefs, modes of behaviour and other non-quantifiable factors which makes the "how much?" question insufficient. It is not an immutable block to be added in, but an adaptive entity that requires adjustment for every line of business, process, asset, and situation. Security should be seen as a factor contributing to the core business and hence increasing reliability; not as a nuisance hindering operational flexibility. It should be managed as an entity penetrating the entire organisation and all its operations, yet individualised as appropriate to every process and asset. Therefore, security

is a concern for the executive and board levels. It is a strategic question. Desired outcomes should be the starting point for making evaluations about what kind of security and at how high levels one wants to have. The company should define its core processes and assets because these determine what is to be secured, from what, how, and for what period of time. One should take an inventory of the current situation; conduct a thorough, yet realistic threat analysis; and on this basis define clear objectives for security management. Objectives should be in line with the desired outcomes, and successful management takes one where one wants to be. Finally, how to ensure the continuation of operations in every situation is the key thought to guide security management. If this is undesirable, there should be a plan to take the operations down and to concentrate on mitigating the consequences.

What one's core business is influences security evaluations. How prone to collapse the business operations are, for instance, in case of a single successful cyber attack and the reputational damage thus done is an aspect to be taken into consideration. For some companies this is the main concern and it can be addressed through effective strategies of resilience, fast recovery and public relations. For other companies this is not enough. For example, the exposure of a nuclear power plant to any kind of attack is close to unacceptable not only because of the importance of power supply, but also because of the disastrous direct and/or indirect consequences the attack may have. Security levels must hence be high and the variety of countermeasures broad. The overall range of possible security levels, as well as that of the associated costs, is wide. The national importance of the business and the value of each line of business to the company, as well as the severity of the potential consequences of something going wrong, are not to be disregarded.

How to set the level of security also depends on the reference object and its importance to the business. Security has multiple faces. Managing security requires that all of these faces are taken into consideration adequately. The list of reference objects includes, for instance, operational reliability, storage and flow of information, intellectual property rights, safety and wellbeing of the personnel,

5 POINTS

▲ **SECURITY INVOLVES** emotions, modes of behaiviour and other non-quantifiable factors

▲ **SECURITY SHOULD** be seen as a factor contributing to the core business

▲ **ONE'S CORE** business influences security evaluations

▲ **HOW TO** set the level of security depends on the reference object

▲ **IT SHOULD** be considered what security does to the business

physical (in)accessibility, and the security of customers and associ-ates. This versatility requires individualised security solutions that still comprise a manageable entity. More-over, it is necessary that security management is aligned with the overall business objectives.

Proportioning the costs of necessary investment to the potential losses caused by a security breach is only one way of making decisions. The calculus, as well as the more applicable yet in itself inadequate risk calculus, is likely to go wrong as security is labile. Decisions made on the basis of experience only reflect the past and are poor in predicting the future. In addition, defining the direct costs (value of stolen property, financial loss, and increasing insurance expenditure) of a security breach

210m
THE TOTAL SALE OF SMARTPHONES GLOBALLY IN Q1 OF 2013

is difficult enough; not to mention the measuring of indirect costs (damage to reputation, lost customer and associate trust, and costs of recovery).

Finally, it should be considered what security does to the business. As an everyday process, it establishes the norm ("the business as usual") and designates devia-tions from it. Security creates a standard. It provides the company with predictability and operational reliability. It enables intervening in deviations by making them vis-ible and also defines what insecurity means. C&L

— This article is printed with prior permission from www. infosecisland.com. For more features and opinions on information security and risk management, please refer to Infosec Island.

Security Intelligence for the Enterprise

Security Intelligence is a very hot topic right now on the "to do" list of CISOs across enterprise space **By Rafal Los**

Here's an inconvenient observation: Of the 20-plus mid-market enter-prises I've spoken to about security intelligence in the last few months, less than five are actively using security intelligence for better defense. What gives? This post will describe for you what I believe it means to extract value from security intelligence. And more important, why I believe three out of four enterprises are still failing to get that value.

Getting Value

As is the case with nearly anything else, having a tool at your disposal doesn't nec-essarily mean you're benefitting from it. Buying a brilliant hammer doesn't make me a master carpenter and all that. But what it does get me is something that requires more work on my part to realize

value. What is this mythical value I keep talking about?

Value is a funny word. Maybe it's more interesting to think about utility, and how we may derive utility from having a resource available to us. Alright, enough word play — let's talk about what it means to get value out of security intelligence in your enterprise.

First off, let's take a quick peek at your enterprise security program. If your organi-zation is without a framework with respect to defending your organisation and its assets, do not read further. Instead, seek out someone who will be able to help you build that framework, call it a security pro-gramme, and come back.

Within the construct of your enterprise security programme, you should have a framework for using tactical intelligence in

such a way that it aids in your decision mak-ing and adjustment processes. The problem here is that roughly half of the enterprises in this mid-market space I've spoken with don't actually have a construct for making tactical adjustments. Another quarter are lacking a solid enterprise security frame-work (otherwise referred to as a "security program"), which means any attempt to bring in tactical intelligence into that mess will likely result in something akin to yell-ing "Shark!" in a movie theater. (I'll let you figure that one out yourself.)

Assuming you have a framework for consuming tactical intelligence — security intelligence — your organisation can now start to incorporate some of those feeds and reports into your daily activities. The prob-lem is, however, there is still a vast chasm between "We have a report!" and "We are

acting on this report!" You see, getting value means converting information into action. To take that a step further: Getting value means converting information you receive into actions you take in a timely fashion, which enable you to make good decisions to protect your enterprise. This is my loose definition, but I think it works.

Value to me means that you're able to convert the information you receive in a timely manner into meaningful actions to defend your enterprise against an imminent threat.

Of the roughly half of the organisations that I've spoken to that break down somewhere in this process, most of it falls apart at the meaningful and timely. They can usually read the PDF that's sent to them, and at some time convert it into action, but it's rarely meaningful, and almost certainly not timely. Let's look at this a little deeper.

Failure to Capitalise

There are any number of reasons (or excuses) why enterprises are failing to realize that value just discussed. They're missing at least one, if not many more, of the criteria that are required to claim value. This is clear. But the major issue from where I'm sitting is, in spite of that failure, budgets are still being widened to include security intelligence as a strategic purchase. This is rather disturbing because you're wasting money, and likely your own valuable resources, in an investment you're almost certain will not pay off.

I've always heard that the only way to fix a situation is to admit that it's happening. In order to find your way back to the highway, often times we simply must admit to ourselves that we're lost and stop and ask for directions. With that in mind I offer my top five.

Here's my assessment of the top five major failures when it comes to getting value from security intelligence for the enterprise:

● Inadequate framework for response. First and foremost, if you don't have a framework for consuming, transforming, and acting upon intelligence you're receiving from outside parties, there is not a snowball's chance you'll actually see value. Sure, they say that even a blind squirrel finds a nut eventually, but if you don't have a framework in place you're hopelessly wasting resources and may actually be causing your organisation harm rather than good. Unusable format. Ever wonder how you can convert that 10-page PDF into quick action? Same here. There is a format that lends itself best to consumption by your organization, and it is your job to find that format. Whether it's a web portal, a PDF, or a XML-based data feed into your SIEM — it has to work for you. (Otherwise, it's working against you.) The copy/paste-from-PDF- to-firewall rule is likely going to slow your organisation down before it speeds you up. Remember this has to be converted to action in a meaningful amount of time.

● Timeliness failure. Sadly, many of the reports I have seen some of these 20-plus organisations receive, come at some regular interval. Maybe it's Monday morning, or mid-week, or twice a month ... either way, if they're not sent in a timely manner — meaning as they're needed — they quickly become irrelevant and are relegated to historical value. This doesn't help you tactically adjust, you're not the TSA here. I'll just leave it at that.

● Unusable information. Information about adversaries and their tactics is fantastic, unless it's not something you can do anything about. Let's say you're a mid-market banking organisation who just received intelligence that your sector is being targeted by "foreign nation-states." I was asked by a client what I would advise they do with a report like that ... to which my answer was an unfortunate shrug of the shoulders. Without detail, these types of reports only seek to cause wasted cycles, and confusion, in my opinion. I know certain peers will disagree with me but that's okay.

● Inadequate resources. Even if everything else is great, and your framework supports a response, you have timely, usable information in a usable format, there is still a good chance the people you're hoping to task with this response activity are busy doing 20 other tasks. You see, even if everything else works out near perfectly, you probably aren't staffed for this type of response, and the intense levels of activity it requires. And that, after all this, may be the root of the problem. Staffing is once again our Achilles Heel in the enterprise.

There you have it, all the reasons why you're probably failing at making use of the security intelligence you are actually receiving. C&L

— This article is printed with prior permission from www.infosecisland.com. For more features and opinions on information security and risk management, please refer to Infosec Island.

PHOTO BY PHOTOS.COM

VIEW**POINT**

STEVE DUPLESSIE | steve.duplessie@esg–global.com
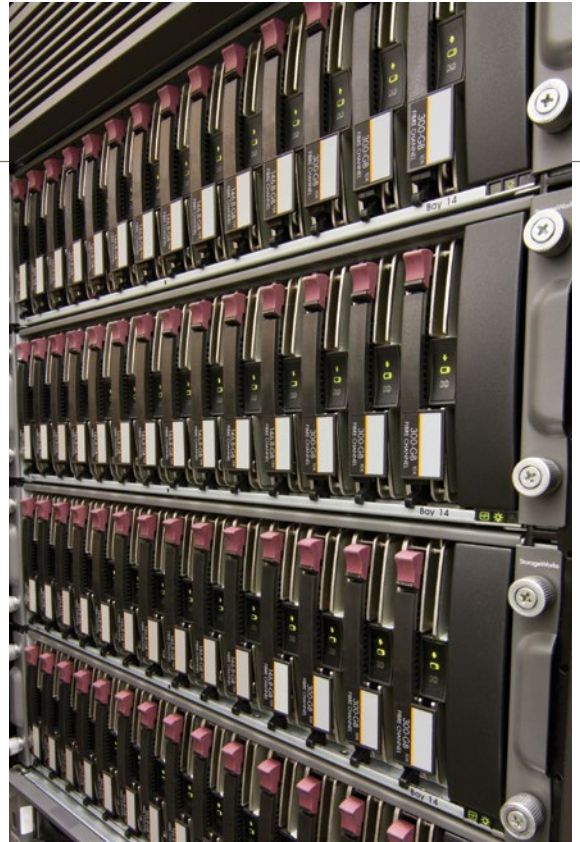
We've Seen This Movie Before
Nothing is ever new in IT, and Big Data is no exception

BIG DATA in 2013 is SAP(ERP) twenty years ago. Or Siebel (CRM) 12 years ago. It's rolling out the exact same way.

1. Users use all sorts of disparate, loosely connected applications to piece meal a solution together. In the pre-SAP days, it was a warehousing system, an inventory system, a manufacturing/flow system, an ordering system, an accounting system, etc. etc.

2. Someone develops an integrated, single stack application that can throw out all the custom home grown, disparate junk systems and provide a single unified, connected pane of glass. In the SAP case, we called it ERP.

3. Advanced IT shops, typically in very large, well-funded companies with strategic vision, jump on the opportunity. They become the early adopters because they know that a successful implementation will provide a distinct competitive advantage to their organisations. These are few and far between.

4. The buzz created by the next great thing gets the mainstream market going. These are the everyday folk who's bosses boss hears about what's happening out there in the world and asks their IT department to get on the train—no matter what that train is, or how capable their organisation is at getting on. (Cloud, anyone?)

5. Companies drink the kool-aid and start spending like drunken sailors. SAP becomes HUGE. Implementations go from dozens to thousands in short order. Each implementation has a massive up front cost (which SAP loves, as well as the ecosystem providers like EMC or HP in this case), and requires an army of services to make stuff remotely work. It takes years to customize the system.

6. 80 percent or more of all those really expensive implementations fail spectacularly—because the issue was never really about the technology (10 percent), it is always about the business processes—or lack thereof. In the case of SAP's rise to glory, the issue was "now that you have spent 20 million bucks over five years to get this implemented,

ABOUT THE AUTHOR:
Steve Duplessie is the founder of and Senior Analyst at the Enterprise Strategy Group. Recognised worldwide as the leading independent authority on enterprise storage, Steve has also consistently been ranked as one of the most influential IT analysts. You can track Steve's blog at http://www.thebiggertruth.com

you need to change the way you do business to fit our software." That's why these implementations died a painful death.

Only after SAP was able to help customers (via partners) to understand that this wasn't a panacea platform that does all the work for you—but a panacea platform to capture and create efficiencies ONCE you re-architected your business outcomes/processes did it gain huge momentum again. And, it never looked back.

In Big Data, I see the same thing evolving. First it's all about the exciting "Gizmo's"—the industry gets fired up and buys Netezza, Greenplumb, Vertica, etc. because they do SOME function wicked fast—but mostly without context of the bigger issues (like "what the hell is big data?").

Then we move on to create a class of super geniuses—in this case "Data Scientists" who can manipulate data so that we can find needles in our proverbial haystacks. You can't find them right now—they are super rare geeks. **C&L**

The greater promise of a greater cloud.

By next year, 41 percent of enterprises are projected to have substantially implemented cloud technology into their practices—up from 13 percent in 2011.

Only 16 percent of companies say they use the cloud for significant innovations, such as entering new lines of business or reshaping their industry.

Today's public, private and hybrid cloud platforms aren't just changing computing models. They're changing *business* models.

On a smarter planet, a few bold thinkers are seeing the cloud not just as a platform for optimisation, efficiency, storage and security, but as an incubator of ideas. They're using the cloud to test, adjust and deploy new innovations, serving their customers better as they develop new services and revenue streams with less effort and expense.

After efficiency lies innovation.

Enterprises that use the cloud can build their reach at a lower cost. After the United States Tennis Association migrated its predictive analytics and mobile infrastructure to a private IBM Smart-Cloud, millions more users of USOpen.org could easily access its news, analytics and live streaming.

And innovating in the cloud can help a business learn in real time. When produce company Blattwerk prepared to launch food trucks, it planned to use mobile scanners to monitor distribution. Building this system in the cloud helped Blattwerk launch its trucks in just three months.

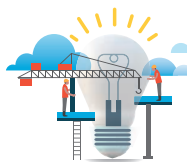### Extending infrastructure to extend ideas.

Forward-thinking enterprises that link their infrastructures to the cloud can focus on new ideas. When a software provider for hotels, PassportScan, enabled its technology on a public cloud platform, it found it could enter a new market. Last year, PassportScan expected its cloud-platform revenues to double.

The cloud beyond the cloud.

When a smarter enterprise uses the cloud to support Big Data and analytics, mobile and social solutions, it can reimagine how it thinks, works and serves customers. Today's enterprise cloud is about more than expanding reach. It's about expanding possibility. To find out more, visit us at **ibm.com/cloud/in**

By 2015, revenues from cloud-enabled innovations are expected to exceed $1.1 trillion— half of it generated by small businesses.

LET'S BUILD A SMARTER PLANET.

O8M082