Opinion | Pg 14
A Cloud Compliance Crisis

Insight | Pg 27
Is Your Data Hack-Proof?

IT NEXT
FOR THE NEXT GENERATION OF CIOs

Are you ready to be a Data Protection Officer?

The Indian draft personal data protection bill requires that every organization handling personal data should have a data protection officer. Are information security professionals the right candidates?

August 2018 | ₹100 | Volume 09 | Issue 03 | A 9.9 Group Publication
www.itnext.in | facebook.com/itnext9.9 | @itnext_

#TheBigPicture

42% of the winners report to a C level

64% of winners work in organizations with IT budget of over 10 crore and above

Come and establish camaraderie with the IT giants of tomorrow

INDIA's FUTURE CIOs
NEXT100
2018

For engagement opportunities, please contact

Mahantesh G	9880436623	mahantesh.g@9dot9.in
Deepak Sharma	9811791110	deepak.sharma@9dot9.in
Prashant Amin	9820575282	prashant.amin@9dot9.in
BN Raghavendra	98453 81683	bn.raghavendra@9dot9.in
Vandana Chauhan	9958984581	vandana.chauhan@9dot9.in

Apply for the NEXT100 today—it could change your life. Go to: www.next100.in

Personal Data Protection: The New Compliance Test

The third parties here are mom-and-pop shops who work for large corporations in multi-tier ecosystem. Making them compliant is not a small challenge

Shyamanuja Das

India has finally come out with its draft personal data protection bill. If you are an information security professional, I assume that you have already gone through the draft and have identified the gaps that you need to fill. If you are part of an organization that has already complied with European GDPR, then at least you are familiar with the concepts and basic steps.

In the recently concluded 19th CIO&Leader Conference, I asked a number of CIOs—some of who also handle security in some capacity—about the preparation for complying with the regulation. It was heartening to know that most B2C companies are sensitized. Some have even created teams to figure out what to do. This is a long way from the state of affairs just a few months back. When I had asked a similar audience, nay, actually all security professionals about Srikrishna Committee white paper that had been released two weeks back, many of them had not even heard of it!

The growing sensitization is good. Because it is the security professionals who will ensure that some of the obligations are met with.

The cover story explores if CISOs or other security professionals would be designated as Data Protection Officers (DPOs) that the bill requires organizations to appoint.

India will face a unique challenge. Unlike in the West, in India, few citizens are worried about privacy. An INR 10 recharge will make people share all their details. The third parties here are mom-and-pop shops who work for large corporations in multi-tier ecosystem. Making them compliant is not a small challenge. Add to that India's track record of enforcement (India is fairly progressive in enacting legislation) and it is going to be a tough game.

My guess is that the sectoral regulators and industry associations in industries like banking, telecom, insurance and mutual funds, will sit together to create some sort of guidelines. I also expect that the CISOs will be mandated to carry out the responsibility of DPO, at least initially.

So, get ready. And also, do not forget to go through the draft bill carefully and offer your suggestions. The government has asked for feedback on the draft bill, which has to be submitted by September 10.

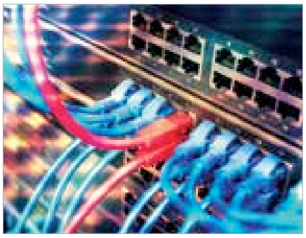
All the best!

AUGUST 2018
VOLUME 09 | ISSUE 03

Content

Are you ready to be a Data Protection Officer?

There will be thousands of new requirements for data protection officers once the Indian personal data protection legislation comes into effect. The IS professionals could be serious contenders to the positions.



ADVERTISER INDEX	
Vodafone	BC

Please recycle this magazine and remove inserts before recycling

IT NEXT
ITNEXT.IN

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

EDITORIAL
Managing Editor: Shyamanuja Das
Content Executive-Enterprise Technology: Dipanjan Mitra

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

SALES & MARKETING
Director-Community Engagement: Mahantesh Godi (+91 9880436623)
Brand Head: Vandana Chauhan (+91 99589 84581)
Assistant Product Manager-Digital: Manan Mushtaq
Community Manager-B2B Tech: Megha Bhardwaj
Community Manager-B2B Tech: Renuka Deopa
Associate-Enterprise Technology: Abhishek Jain

Regional Sales Managers
South: BN Raghavendra (+91 9845381683)
North: Deepak Sharma (+91 9811791110)
West: Prashant Amin (+91 9820575282)

Ad co-ordination/Scheduling: Kishan Singh

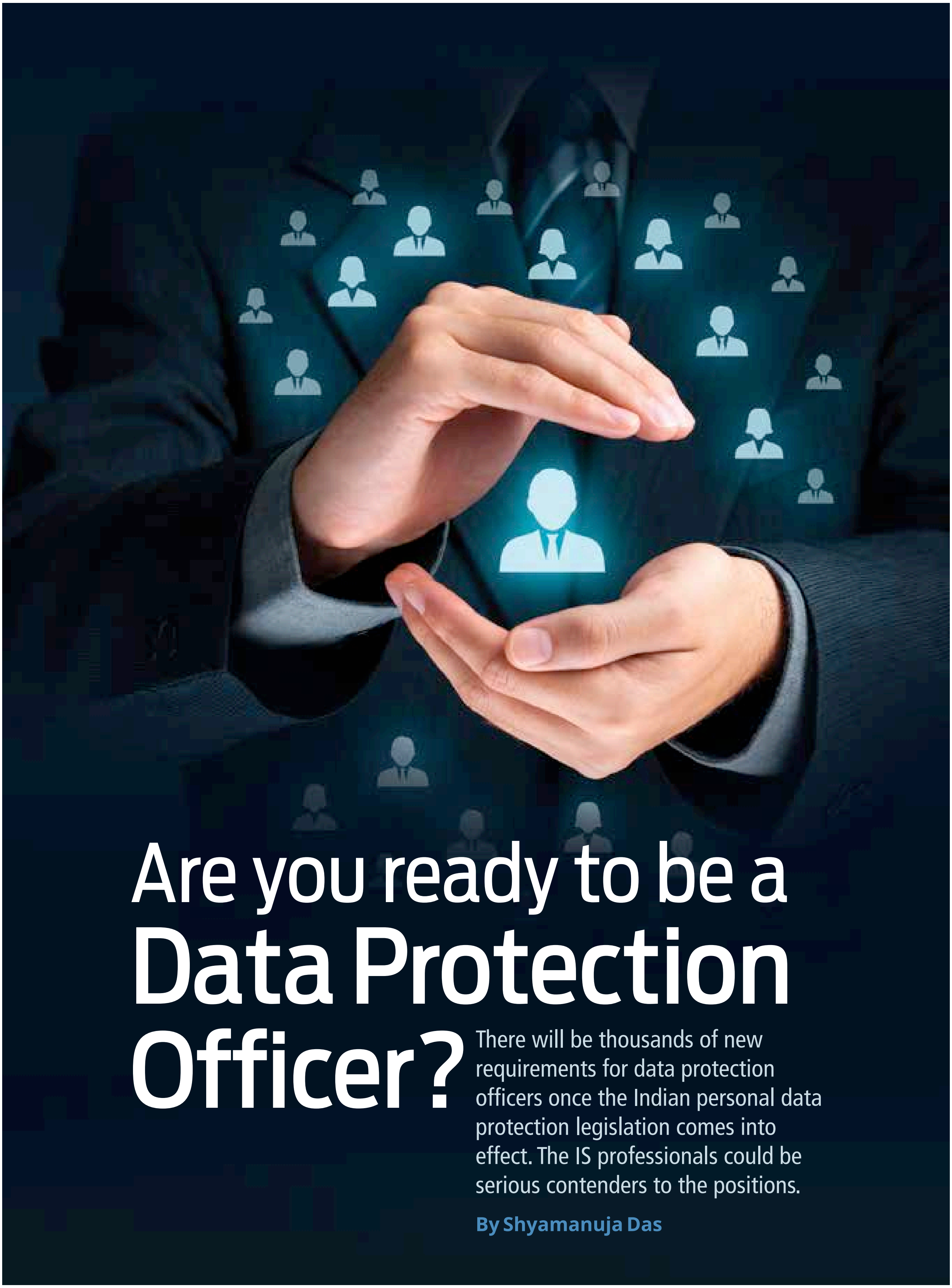
Manager - Events: Naveen Kumar
Manager - Events: Himanshu Kumar

PRODUCTION & LOGISTICS
Manager Operations: Rakesh Upadhyay
Asst. Manager - Logistics: Vijay Menon
Executive Logistics: Nilesh Shiravadekar
Logistics: MP Singh & Mohd. Ansari

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121- Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091

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

Editor: Vikas Gupta



Are you ready to be a Data Protection Officer?

There will be thousands of new requirements for data protection officers once the Indian personal data protection legislation comes into effect. The IS professionals could be serious contenders to the positions.

By Shyamanuja Das

Justice BN Srikrishna committee formed to draft India's privacy legislation has presented its draft bill, called Personal Data Protection Bill 2018. The draft bill has been prepared after public consultation through a discussion white paper. The white paper itself was prepared after reviewing such privacy regulations across the world, with a lot of provisions matching point by point, with the most well-known of them all, the European Union's General Data Protection Regulation (GDPR).

The bill, when it becomes law, will require the organizations dealing with personal data of individuals (called data fiduciary by the bill) to comply with a number of provisions to ensure that the data principal (whose personal data is being dealt with) has reasonable control over how his/her data is being used. A significant way in which it differs from GDPR is that the Indian draft bill does not acknowledge the data principal to be the 'owner' of that data explicitly. One of the major practical implications of this difference is that the Indian data fiduciaries are not required to ensure data erasure—an important and difficult-to-achieve requirement of GDPR.

To ensure that the privacy requirements are adhered to and the obligations in terms of the rights of are met with, the bill (like other privacy legislations) has an approach called 'privacy by design'. The Indian draft bill, in its Clause VII (36) explicitly mandates that every data fiduciary should appoint a Data Protection Officer.

The Data Protection Officer (DPO), while generally advising the data fiduciary on how to meet with the compliance requirements of the bill, will also be the point of contact of the regulators as well as the data principals (the citizens whose data is being processed). It allows the DPO to carry out any other responsibilities of the company. While there's nothing in Indian draft bill that explicitly mentions about any role or reporting structure that could be in conflict with the DPO role—like for example RBI and IRDA mandating that CISOs in banks and insurance companies respectively should not report to the CIOs—it is understood that the data fiduciaries have to ensure that in the best interest of their ability to meet the compliance requirements, the DPO role should be as independent as possible of any regular functional role.

Who is suitable for a DPO role?

So, who should be a good candidate for a DPO role? And are information security professionals like CISO a good choice to carry out the responsibility?

To answer the question, we must look at the role specified by the draft bill and examine what skills, knowledge and experience can be useful in fulfilling the duties and if the Information Security (IS) professionals could fit into the role.

Here are the specific roles mentioned by the draft bill:

- **Providing information and advice on fulfilling obligations:** This is more about knowledge of the legislation and experience. It can be carried out by any professional who has knowledge and experience. This could be a legal professional, IS professional or any other business professional who has worked in compliance.
- **Monitoring data processing activities:** Typically, IS or quality professionals would be the best suited to carry out this responsibility.
- **Providing advice on and carrying out impact assessment:** Again, a quality or IS professional should be able to effectively discharge this responsibility.
- **Setting internal mechanisms:** Operations, Quality and

Process professional are the best people to do this. Those IT/IS professionals with considerable experience in process/project management can also be good candidates.

- **Providing assistance to Data Protection Authority:** Typically, legal professionals can do this role better as it may require them to continuously assess the validity of the request and figuring out how to meet them with minimum effort.
- **Act as point of contact for data principals:** Traditionally, none of the roles in organizations that are good breeding grounds for DPOs are customer facing roles. So, it is anyone's guess. Depends on the individual.
- **Record keeping of data processing process:** This role requires the DPO to keep a record of when and how data is collected, processed, stored and erased. Any good process professional can do the role but IS executives are especially suited for this role, as most challenges regarding technology will arise out of this.

In industries that are regulated and the sectoral regulators have some kind of requirements of data safety/protection, those responsible for complying with the regulation should be an automatic choice for carrying out the DPO responsibility.

Global Trends

What kind of people are handling the role in large global companies, especially those operating significantly in more mature markets with democratic governments?

To get a cue, we researched the top Fortune 500 companies to find out the trends. Here are some of the findings.

In many large organizations, the role falls under the Compliance function, with a Chief Compliance Officer. In many organizations, the Chief Compliance Officer himself/herself is the DPO accountable. Take Volkswagen, the 7th largest listed corporation according to Fortune 500 2018. The automotive major has a Chief Compliance Officer Kurt Michels who is overall responsible for privacy. Same with Toyota, whose North American business has a Chief Compliance Officer Jacqueline Thomas responsible for data protection and privacy.

But in most large organizations, most notably those who deal primarily with consumer data, have had Chief Privacy Officers for long who are responsible for privacy policies, implementations with responsibilities that include compliance, practices, tech and more. World's largest corporation, Walmart, has a Chief Privacy Officer Jonathon Avila, who is responsible for privacy and data protection. So, has Royal Dutch Shell, where a Group Chief Privacy Officer, Helen Graham carries out the responsibility. BT, Microsoft, Apple and a host of tech and information-centric companies have such positions. These positions have been there much before the recent wave of data protection legislations.

Recently, most significantly, post GDPR, many have appointed senior executives explicitly carrying the designation of Data Protection Officer/Chief Data Protection Officer/Group Data Protection Officer. Insurance major Allianz (38th in Fortune Global 500) has Dr Philipp Raether who is designated as Group Chief Data Protection Officer. BNP Paribas, the 44th largest global corporation going by Fortune Global 500, has given this responsibility to its Chief Cyber & Technology Risk Officer, Ramy Houssaini.

Most of these positions—be it Chief Compliance Officer or Chief Privacy Officer or Data Protection Officer—are held by legal professionals. Walmart's Avila, Shell's Graham, Volkswagen's Michels, Apple's Jane Hovarth, Allianz's Dr Raether, BT's Emila Chantzi are all attorneys.

The notable exceptions include BNP Pariba's Houssaini and the Chief Privacy Officer of Microsoft (71st largest corporation in Fortune Global 500) Brendon Lynch. Houss-

As the Bill specifies it

(The relevant clauses from draft Indian Personal Data Protection Bill 2018)

SECTION 36

Data Protection Officer. —

(1) The data fiduciary shall appoint a data protection officer for carrying out the following functions:

- providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;
- monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;
- providing advice to the data fiduciary where required on the manner in which data protection impact assessments must be carried out, and carry out the review of such assessment as under sub-section (4) of section 33;
- providing advice to the data fiduciary, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under section 29;
- providing assistance to and cooperating with the Authority on matters of compliance of the data fiduciary with provisions under this Act;
- act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary pursuant to section 39 of this Act; and
- maintaining an inventory of all records maintained by the data fiduciary pursuant to section 34.

(2) Nothing shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary, in

addition to the functions provided in sub-section (1) above. 21

(3) The data protection officer shall meet the eligibility and qualification requirements to carry out its functions under sub-section (1) as may be specified.

(4) Where any data fiduciary not present within the territory of India carries on processing to which the Act applies under section 2(2), and the data fiduciary is required to appoint a data protection officer under this Act, the data fiduciary shall appoint such officer who shall be based in India and shall represent the data fiduciary in compliance of obligations under this Act.

SECTION 34

Record-Keeping. —

(1) The data fiduciary shall maintain accurate and up-to-date records of the following—

- important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 11;
- periodic review of security safeguards under section 31;
- data protection impact assessments under section 33; and
- any other aspect of processing as may be specified by the Authority.

(2) The records in sub-section (1) shall be maintained in such form as specified by the Authority.

(3) Notwithstanding anything contained in this Act, this section shall apply to the Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority which is "the State" under Article 12 of the Constitution.

saini is a tech professional while Lynch is a career risk and privacy professional. Interestingly, Microsoft announced appointment of a EU Data Protection Officer, just before GDPR kicked off. Steve May, the person appointed to that position too is a business executive, not from legal profession.

So, here is the summary:

- Many large corporations already had Chief Privacy Officers. Some of them are appointing geography specific DPOs. Indian draft bill also explicitly mandates that non-Indian companies should have a DPO based in India.
- Some have appointed Data Protection Officers now.
- Most of the positions—irrespective of what it is called and how broad/narrow their scope of work is—are from legal backgrounds. There are notable exceptions, though.

Indian companies, who have to comply with GDPR and other country specific regulations also have started appointing their privacy/data protection officers. As can be expected, most of them are IT/BPO companies. Interestingly, these executives appointed by Indian companies have a wide range of different experience and backgrounds that they bring in.

Infosys' global DPO, Srinivas Poosarla, is a quality professional. So is NIIT's recently appointed DPO Vivek Kumar. Among those with IT/IS background include L&T Infotech's DPO Vikarm Patil, and Quatrro's Chief Privacy Officer Ganesh Viswanathan. Viswanathan is the company's CISO as well. Ramco's Global Chief Data Protection Officer, K Satish Kumar is a legal professional. Indians seem to be more open about the background of their DPOs. But there's a corollary there: so far, it is the IT companies that have appointed people to these positions.

Is there a path for IS professionals?

As can be seen from global practices, it is predominantly legal professionals who dominate the DPOscape. Does it mean that the IS professionals do not have a chance?

We do not think so. This is why.

One, this is the time when privacy regulations are evolving. Most organizations want to do it correctly, and somehow comply with it, as soon as possible. At this time, what they need is people who can understand the legalese and defend them, in case that is required. That explains why so many legal professionals are appointed. As there's more understanding and appreciation and interpretation of clauses ceases to be an everyday job, organizations may switch over to people who can get the work done, can continuously enhance the capability and ensure that newer targeted attacks to steal personal data get effective thwarted. CISOs/IS professionals would fit the role far better

Two, in India, there are just not too many legal professionals who are well versed with technology. So, many Indian companies will go for legal consultants even as they go for tech people to carry out the actual tasks to ensure that the non-compliance does not happen. It's primarily a tech job.

The fact is this job requires knowledge of law, tech and prior experience with compliance. Those legal professionals who familiarize themselves with tech or the IS professionals who familiarize themselves with finer nuances of the law, both have opportunities before them.

Like the CISO role, it is about constant battle. If you love that challenge, this is something you should seriously consider.

A practical tip: Look at the job descriptions of the people in LinkedIn or in positions advertised anywhere in the world. Here's one such advertisement by Cathay Pacific: https://careers.cathaypacific.com/jobs/data-protection-officer-5790049

That will give you a fair idea about what organizations are looking for. ■

India's draft data protection bill: What's the deal?

What you must know about India's draft personal data protection bill – the genesis, the controversy and the essential features...

On Friday, Justice BN Srikrishna, chairman of the nine-member committee set up by the government to draft a personal data protection bill, handed over its 213-page report, *A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians*, along with the draft data protection bill to the Minister for Information Technology Ravi Shankar Prasad.

A nine-judge constitutional bench of Supreme Court had delivered a historic judgment on August 24 last year recognizing right to privacy as a fundamental right and urged the government to bring in data protection legislation. "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but also from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection," Justice DY Chadrachud, part of the bench had said, in his judgment.

Justice Srikrisha committee, formed just prior to that judgment (in July 2017), had released a white paper in November 2017 with major points under considerations under the proposed bill and had asked for stakeholder comments.

The draft bill is prepared taking into account the inputs received, according to Justice Srikrishna. However, unlike some other public consultation processes like those of the Telecommunications Regulatory Authority of India (TRAI) which makes the stakeholders' comments public, the panel chose not to release them publicly, leading to criticism that it was non-transparent. However, the report does include a dissent note by one of the members, Rama Vedashree, the CEO of Data Security Council of India (DSCI), the only such dissent note.

The release of the report was marked by high drama. In an interview post the release of the report and the draft bill, Justice Srikrishna accused RBI of 'jumping guns, for its notification on data residency requirements for payment data in April and calling the release of TRAI's own version of data privacy guidelines released just a couple of days earlier as 'one-upmanship'.

On social media, this first step towards a personal data protection bill was welcomed by many, even though experts perceived it as a 'weak' piece of legislation. The prime accusation was it leaves a lot of scope for government to control personal data the way it wants. Data localization provision attracted the maximum criticism while many discussed how the bill has left scope for Aadhaar to use personal data the way it wants. On its part, the committee suggested amendments to Aadhaar Act, but did not get into further details as "it is with the Supreme Court."

Main Features

Like most of the policy and legislation on data protection the world over, the draft Indian Data Protection Bill 2018, recognized the rights of the citizens on their personal data.

Some of the major features of the bill are as follows:

- Personal data to be processed only for purposes that are clear, specific and lawful; the purpose should be communicated to the data principal (whose personal data is in question) by the data fiduciary (the entity that determines the purpose of processing personal data) at the time of collection or in a reasonable time if it is not collected directly from him or her. A data fiduciary is the equivalent of data controller in GDPR while a data principal is the equivalent of data subject.
- The bill makes consent of data principal necessary to process any personal data, while allowing certain exceptions.
- The bill also talks of rights of data principal—right to access, right to correct, right to data portability.
- The bill then goes into ways and means of ensuring this data protection by imposing certain checks and balances on the data fiduciary which it calls privacy by design (process, technological, organizational changes needed to ensure data privacy). It also explicitly deals with security safeguards, obligations in case of a breach, need for audits as well as appointment of a data protection officers
- Data protection officers will be responsible for compliance as well as act as the point of contact for the individuals for raising grievances.
- It also specifies conditions of transferring data across organizations (third party) and across political boundaries of India.
- It also articulates the exceptions and certain special rights of the government in national interest. Processing of personal data for journalistic or domestic purpose are exempt from complying with these.
- The bill specifies the scope of a regulatory body, Data Protection Authority of India, which the government will notify.
- The penalties (INR 5cr or two percent of global annual revenue, whichever is higher) in case of failure to comply with any of the requirements.
- All anonymized data will be outside the scope of the provisions in the bill.
- The bill, when passed, will necessitate the need to amend existing Acts such as Right to Information Act, IT Act and Aadhaar Act. ■

> On social media, this first step towards a personal data protection bill was welcomed by many, even though experts perceived it as a 'weak' piece of legislation. The prime accusation was it leaves a lot of scope for government to control personal data the way it wants. Data localization provision attracted the maximum criticism...

8 differences between Indian Data Protection bill and GDPR!

GDPR is not just stringent in penalties, it gives far more rights to the citizens

The European General Data Protection Regulation (GDPR) has almost become a common noun for personal data protection regulation, not just for the stringent provisions that it contains but also for comprehensiveness of the issues that it addresses.

The Indian panel created to draft a data protection legislation, under Justice BN Srikrishna has referred to GDPR repeatedly in a whitepaper that it released in November last year as well as the report that it submitted last week, along with the draft Personal Data Protection Bill 2018.

While most of the areas such as having a clear purpose of processing of personal data, consent, other rights, appointment of Data Protection Officers in organizations are taken directly from GDPR provisions, there are a few differences too.

Presented here are ten of the

most important differences between the two. Of course, GDPR is not an Act; individual member nations have enacted their own legislations based on GDPR. They could only add to it.

To some extent, the comparison between GDPR and Indian draft bill, hence is a bit of that between apples and oranges, but only when one gets into the language and enforcement provisions.

We avoid getting into that and analyze only areas where the stances are different on a specific issue.

Please note that the citizens whose personal data is being processed are called 'data subjects' in GDPR terminology and 'data principals' by Indian draft bill. Similarly, entities that process the personal data are called 'data controllers' by GDPR while being referred to as 'data fiduciaries' by the Indian draft bill\`

Please note that the citizens whose personal data is being processed are called 'data subjects' in GDPR terminology and 'data principals' by Indian draft bill. Similarly, entities that process the personal data are called 'data controllers' by GDPR while being referred to as 'data fiduciaries' by the Indian draft bill.

Here are the eight differences:

1. Unlike in GDPR, Indian draft legislation does not require the data fiduciary to share the names and categories of other recipients of the personal data with the data principal.
2. There is no obligation on data fiduciary to share with the data principal for how long the data will be stored while collecting or at any time, as GDPR mandates.
3. The data fiduciary does not need to share the source of the personal data to the data principal in case the data has not been collected from him/her which is an explicit requirement in GDPR.
4. Unlike GDPR, there is no requirement that the data fiduciary share with the data principal the existence of automated decision making, including profiling.
5. GDPR requires that the data subject (data principal) is provided with a copy of data undergoing processing.

   The Indian legislation mandates a summary of that data to be shared, with no definition of what that summary is.
6. **One of the biggest differences is that in India, a citizen has not been given the right to demand his/her data to be erased. Data reassure, which is an article in itself in GDPR does not even find a mention in the Indian draft bill.**
7. In case of a breach, there's no requirement by Indian draft bill to share it with the data principal; rather, the data protection Authority shall determine whether such breach should be reported to the data principal. This is also in contrast to GDPR provisions.
8. The provision that has attracted the most criticism—as well as the only dissent note from one of the members—is the issue of where the personal data resides. "Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies," says the bill. The draft bill also mentions that the Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

GDPR leaves this to specific countries most of which have chosen to allow free flow of data, though Germany and France require personal data to be resident in their countries. A few others like Bulgaria have very specific requirements like gambling data to be stored in the country. Globally, many countries require government data to be stored in their countries. Today, that is the requirement in India too. Australia, for example, mandates that the health data should be stored inside country. This is the most contentious issue.

Overall, while the whole concept of GDPR starts with the premise that the ownership of data must belong to the data subject, Indian bill does not even provide that!

Overall, Indian bill is seen to be a diluted version of GDPR, with lesser power for the citizens! ■

P Jayakrishnan draws lessons on life from his patch of green

Go Green!

NEXT100 Winner 2016

P Jayakrishnan, CIO, Muthoot Pappachan Technologies, shares his passion for gardening

"I've always felt that having a garden is like having a good and loyal friend."
– C.Z. Guest

"The love of gardening is a seed once sown that never dies."
– Gertrude Jekyll

Gardening has been a passion with me since childhood. I remember vividly the genesis of my interest. My father gifted me an Orchid Sapling on my 7th birthday. At first, I was taken aback. I was expecting a toy but received this. What would a 7-year-old do with a sapling?

After my initial apprehension I slowly started tending to it. I used to water it as soon as I returned from school. I was curious to see when it would flower. From that small beginning, I now have a large collection of different varieties of plants in my garden.

In 2014, we moved to a larger house with ample area. The barren land adjacent to my house soon turned into a beautiful garden, of course with considerable effort. I have planted various kinds of fragrant flower, vegetables and even a few fruit trees too. My joy knows no bounds when I enter my garden. I dig the earth and I manure it. I love the smell of dry earth when it is watered. I weed and hoe the plants. I prune the hedges. I sow seeds and I water the tender plants. I happily watch the seeds germinate, grow and sprout. I feel a sense of utmost satisfaction when I see a new flower in my garden. Tending of delicate plants, nursing of flowers, trimming the twigs artistically and preparing and weeding of flower beds afford the greatest delight to me. The time spent in my garden tending to the plants is my greatest stress-buster.

My brother-in-law has a small farm on the out-

P Jayakrishnan

Snapshot

P Jayakrishnan is CIO at Muthoot Pappachan Technologies. He is a NEXT100 Winner of 2016. He has held several leadership positions within the Muthoot Group. He has done his MCA from Madurai Kamaraj University and is certified in IBM Mainframes.

skirts of the city. It is now a fully functional organic vegetable farm. Some weekends and holidays I join in to help him in cultivation and nurturing the organic vegetable plants. Majority of the vegetables required for my home are sourced from this farm. It gives me immense pleasure when I see these vegetables land up on our table in various beautiful dishes cooked by my wife. I feel as if I'm striking a blow for the organic movement in our country albeit in a small way. Of course, the bonus is that I'm immensely proud that my family gets to eat healthy too!

I use the usual gardening tools, such as shovel, hoe, fork scissors, pruning knives, etc., in my garden.

It has been my experience that gardening and taking care of plants is in a sense a microcosm of the IT services and software development lifecycle. Both require what I call the 3 P's – Patience, Persistence and Perseverance. I would like to believe that if I have inculcated any of these qualities in me at my workplace, it is through my love for gardening and plants. When we plant a seed, we don't expect it to grow from the very first day itself. It all begins with a seed and the vision of someone willing to wait. You water it, fertilize it, nourish it and all the time carefully tend it lovingly, waiting patiently for the fruits of your efforts. You continue the cycle for some time patiently and persistently till finally one day a miracle happens. A little green shoot sprouts from the barren ground. A career in information technology is no different. You chip away little by little, patiently and persistently, and you get the fruits of your efforts.

A career in IT needs nurturing like gardening

Green IT initiatives aim to minimize the negative impact of IT operations on the environment by designing, manufacturing, operating and disposing of computers and computer-related products in an environment-friendly manner. Someone who loves plants is someone who cares for the environment. He/she will incorporate those processes in their workplace. They will be the people who will think twice before printing, who will recycle paper, those who will employ lean processes in their day to day functioning.

I believe that gardening is a great way to teach your children about ownership and responsibility. It's a good idea to get them their own tools. We should allow them to oversee their little patch of earth. It will demand their attention on watering, weeding, and harvesting. Gardening also teaches children two universal truths:

1. To sustain themselves in their environment
2. Resources are not infinite, and it needs to be cultivated■

As told to Dipanjan Mitra, Team ITNEXT

A Cloud Compliance Crisis

Mark Hickman, Chief Operating Officer, WinMagic examines the findings of recent research which suggest compliance woes are putting the brakes on cloud computing's onslaught

Almost every enterprise is using the cloud in some way, whether for infrastructure services, or to provide software-as-a-service applications to users. For some time, confidence has been growing in the cloud's role in IT infrastructure, to the point that we are hearing increasing talk of serverless computing – where a company places its entire infrastructure in the cloud, which dynamically expands and contracts resources to meet business needs.

In the future, serverless computing may become a reality. But for now, IT staff continues to battle with the challenges of managing the hybrid environments they already have, rather than feeling able to push everything to the cloud. These complex hybrid environments often include multiple operating systems and cloud service providers, as well as increasingly common use of virtualized servers and hyperconverged infrastructure (HCI).

WinMagic recently conducted research to try and establish whether companies are getting the benefits they want from cloud technology and what, if anything, is holding them back from greater use, maybe even slowly moving towards this new serverless computing world.

There were some really interesting findings. The role good security and compliance policies play in realizing the business benefits were clear; 87% ITDMs surveyed said they limit their use of the cloud because of the complexity of managing regulatory compliance.

Many companies fear compliance is balanced on a knife edge and having a hybrid infrastructure with multiple cloud vendors heightens the risks of falling foul of regulatory requirements, such as those imposed under the new General Data Protection Regulation. A quarter (24%) said, it meant as a result, they only work with a single cloud vendor in their infrastructure, rather than exploit the benefits multi-cloud environments can provide like cost effectiveness, flexibility, reliability, security and avoiding vendor lock-in.

The survey by Viga of ITDMs in Germany, India, the UK and US, noted that 63% felt the need to use multiple infrastructure management tools was also a hugely restricting factor in their use of multiple cloud vendors. This is hardly surprising as, the more tools you have, the more complexity and points at which security and compliance processes can break down are introduced. ITDMs realize this, with over a quarter (28%) stating they would "not be completely confident" IT systems met all the required processes and standards if an aud it was called "today" and 7% went as far as to say there was "a high risk of them failing."

When you get it right, the magic happens!

But there are companies that manage to overcome these challenges by using platform-agnostic management tools. When they do, it enables them to implement solid security and compliance policies across on-premises and cloud providers in a way that treats the hybrid infrastructure as a single composite unit over which encryption, access rights, data protection and data sprawl can be effectively and seamlessly managed. That ability to take a holistic view of compliance increases confidence, and brings additional tangible business benefits:

- 63% improved the efficiency of their systems
- 57% now had enforced compliance across the infrastructure
- 56% say they are more secure
- 32% have made measurable cost savings
- 30% believe their risk exposure is lower

The pain, stopping the gain

The pain caused by poor proprietary management tools, is leaving companies restricted on their infrastructure choices and places them at greater risk of regulatory fines. But poor security compliance is so much more dangerous, putting company data at risk of data breaches, both accidental and through theft, by hackers or even employees. The reality is that both are entwined – you cannot achieve good compliance without management tools that are fit for the purpose in mixed operating system, multi-cloud environments.

Good security management tools won't just help you understand and visualize the overall estate, they'll help you improve productivity and manage compliance through enforced encryption, virtual machine management, password controls and key management. Critically, they will also enable the kind of reporting that will demonstrate that you are following the requirements of regulators and the law to the letter.

Reduce the burdens and worries

The most productive way to pursue a multi-cloud mixed infrastructure and achieve all the benefits that come with it, is to invest in tools that can manage the whole estate and ensure its security and compliance. Proprietary tools may claim to offer the "best solution" for the management of their platform, but you need to manage beyond the single vendor. You want the benefits of a multi-cloud mixed environment – by their very definition proprietary tools fall short of the task you need them to do. And trying to navigate a collection of management tools will add to your IT burdens, inevitably leading to the kinds of human error that expose you to data breaches or audit failure, and keep you in a constant state of worry. And, as we saw earlier, ITDMs say it halts the adoption of the very cloud technologies they want to exploit.

The pain caused by poor proprietary management tools is leaving companies restricted on their infrastructure choices and places them at greater risk...

Without a doubt, the cloud is proving its value to enterprises. But we need to address the management of mixed and multi-cloud infrastructures if we are to overcome the compliance crisis that exists, and have the confidence, as ITDMs, that we can achieve the infrastructure we desire, without compromise. ■

The author is Chief Operating Officer, WinMagic

Stop Waiting To Make The Right Cloud Choice; Start With Busting Three Myths

CIOs can set up their enterprise for the next decade of success only if they get more buy-in across the board to overcome outdated cloud migration myths

By Vaibhav Gawde

CIOs are now tasked with unlocking new growth opportunities, and due to this expanded remit, the smarter bunch of CIOs constantly keep an eye out for ways in which they can empower their organizations to innovate faster and better. Cloud infrastructure, popularly known as Infrastructure as a Service (IaaS), is one such avenue that's finding more traction with the CIO community.

77% of senior IT executives in India believe cloud infrastructure makes it easier to innovate and 78% think that IaaS delivers exceptional operational performance, be it in terms of speed or availability, according to Oracle's recent cloud infrastructure market survey. Further, 74% of respondents stated that moving to IaaS has significantly cut the deployment time for new applications and services. In addition, 75% agree that IaaS should be a part of any enterprise cloud strategy.

One commonly stated obstacle for a move to the cloud is internal opposition. Concerns are around the migration – that it could be expensive, time-consuming and complex – which are misconceptions to a great extent.

CIOs can set up their enterprise for the next decade of success only if they get more buy-in across the board to overcome such outdated cloud migration myths. This becomes all the more important given how innovative new technology makes it further easier to migrate to cloud. 71% of senior IT executives think that companies not investing in cloud infrastructure will struggle to keep up with those using it. Clearly, organizations cannot afford to fall behind in this journey.

Start with busting these 3 common cloud myths:

Myth 1: Complexity

A number of respondents expressed concern over the complexity of migrating existing systems to a cloud infrastructure platform. However, in principle, there's still a significant gap between the complex, custom enterprise datacenter and the generic cloud environment, with most companies having made large investments in their enterprise datacenter.

With the help of new tools, you can now replicate your on-premises environment to one that's hosted on the cloud. Just with the push of a few buttons, the time and investment required in the past to rewrite legacy applications and map the complex web of compute, storage and networking is eliminated. There's no such thing as 'not being ready' anymore. You can move even your apps seamlessly to the cloud.

> Just with the push of a few buttons, the time and investment required in the past to rewrite legacy applications and map the complex web of compute, storage and networking is eliminated. There's no such thing as 'not being ready' anymore

Not just non-critical functions such as dev/test environments, it's fairly easy and simple to even move mission-critical processes seamlessly to the cloud, sans interruption with new migration solutions, empowering organizations to quickly transform their businesses and realize the benefits of the cloud.

Myth 2: Resource Crunch

Another common apprehension is that there's not enough human bandwidth or skills to manage the cloud transition. In reality, cloud can help businesses plug gaps better when there's scarcity of IT talent.

Thanks to new cloud services that enable apps to be moved with just the click of a button, without any need to rewrite app codes, the IT team is bound to save time and hassle.

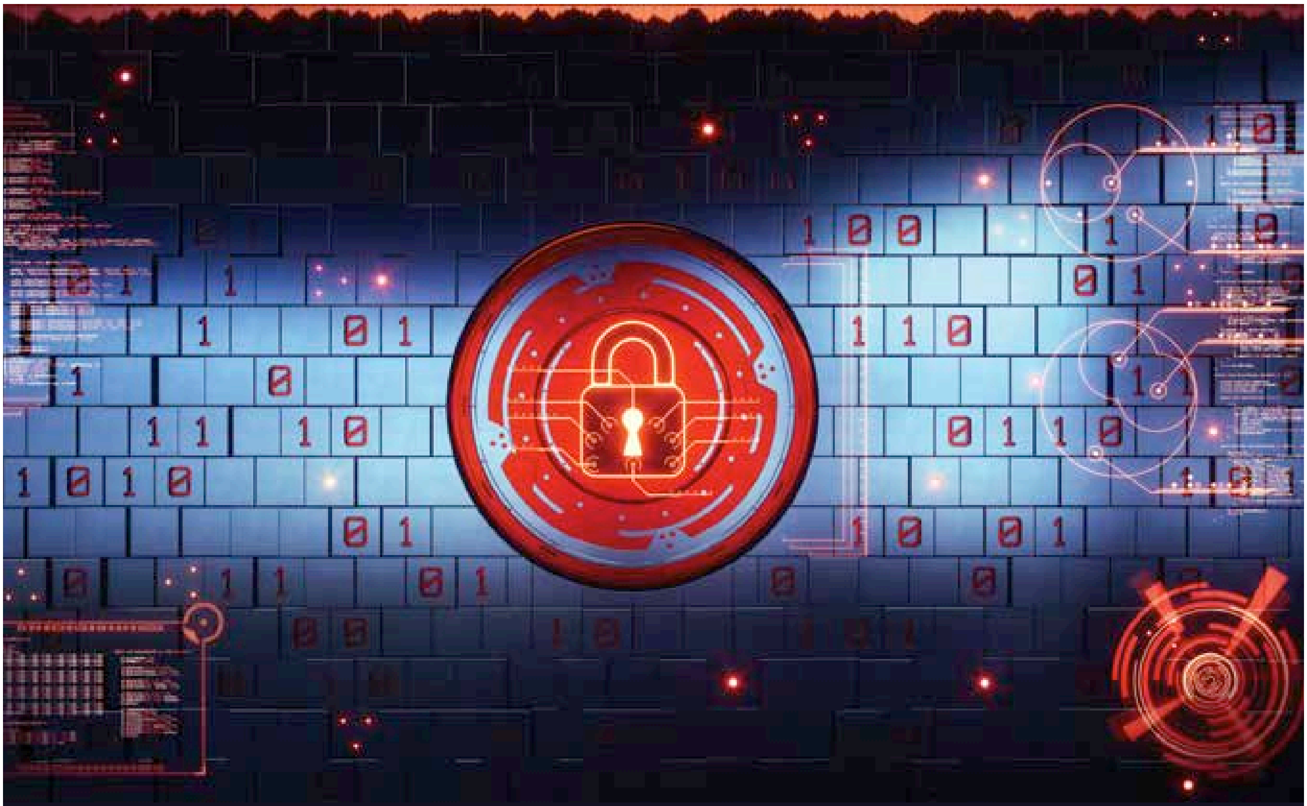
With cloud, developers are able to work faster, continuously and be more cost-effective while developing apps. Research also highlights that moving to cloud infrastructure significantly cuts deployment time of new applications and services and reduces maintenance costs.

Myth 3: Technology Obsolescence

This is another popular myth, that cloud solutions could change with time, making investments outdated. However, the whole point of moving to cloud is to stay current – i.e. leverage the latest innovations so you are up to date. Further, the opportunity to move applications into the cloud extends the life as well as value of investments made in the past. In addition, you stand to gain all the cloud benefits like security, uptime and availability.

This is an opportune time for CIOs to stop waiting and make the right cloud choice. The clock is ticking! ■

The author is Head - Solution Consulting, Oracle India



C-suite Perspectives On Trends In The Cyberattack Landscape, Security Threats And Business Impacts

Most of the C-suite executives rank improvement of information security and business efficiency as their main goals

By Nikhil Taneja

C-suite executives understand that to transform their businesses, they must embrace the integration of new technologies. Most rank improvement of information security and business efficiency as their main goals. Globally, executives indicate they are ready to embrace automated processes as part of their security protocols.

Securing Networks is Critical to Protecting Brand Reputations

Executives are very concerned about the impact that security threats can have on business performance, pointing to the potential loss of customers, brand reputation and operational productivity. Many adjust budget priorities to better secure networks and prevent attacks. Events that most influence how executives view their companies' security vulnerabilities include high-profile data breaches and nation-state attacks, cyberattacks on their organizations and governmental regulations.

Risk Management Calculations Affect Security Investments

C-suite professionals actively monitor what's happening with their networks. They face tough choices when deciding where to invest resources to propel their businesses forward. Reported instances of ransom attacks jumped dramatically over the past two years. As the demand for security professionals outpaces the supply, executives are increasingly looking to carriers or ISP/CSPs to manage security.

Network Security Concerns Vary by Industry

The impact of attacks on corporate networks can vary depending on the industry in which companies compete. Manufacturers who have long embraced automation as a means to boost efficiencies and production reported plans to integrate automation in security measures with a corresponding shift in their IT budgets.

The finance/insurance industry continued its forward-thinking use of technology as a business enabler and reported plans to move operations to the cloud while continuing to focus on digital transformation. The retail/wholesale industry is concentrating on managing the increasing complexity of the IT networks, digital transformation plans and the adoption of Internet of Things (IoT) as a means to better serve customers.

> C-suite professionals actively monitor what's happening with their networks. They face tough choices when deciding where to invest resources...

Securing the Digital Transformation

Corporations are continually looking for ways to increase productivity and efficiency. Taking advantage of technology advances in their networks is a proven way to be more agile while reducing costs.

Customers, employees, vendors and partners use mobile applications, chat bots, online portals, email and other tools to interact with brands daily. Every touchpoint adds a layer of complexity to the network that can introduce new, risky attack vulnerabilities. C-suite executives understand that, to transform their businesses, they must embrace the integration of new technologies while at the same time protect data privacy.

According to a survey conducted and responses sought from senior leaders from the Americas (AMER), Europe and the Middle East (EMEA) and Asia-Pacific (APAC):

- 70% AMER & EMEA executives and 80% of APAC executives are greatly concerned about data privacy
- 47% recognized that digital transformation activities place pressure on their organizations' security planning and investment strategy
- 32% of AMER, 13% of EMEA & 18% of APAC executives rank new revenue sources as top 3 organizational goals
- Most organizations host 25% to 50% of their business applications in the cloud
- 96% were "very" or "somewhat" concerned about network vulnerabilities
- 71%of executives reported shifting more of their network security budget into technologies that employ machine learning and automation
- About 25% said that the focus of their budgets remained unchanged in this time period
- Most organizations worry about huge bandwidth cost by public cloud providers due to DDOS attacks
- Globally, nearly four in 10 executives trust automated systems more than humans to protect them against cyberattacks

A secure climate for customers

Corporations' networks are the lynchpin of interactions with customers who expect responsive applications, fast performance and above all, protection of their data. The foundation of customer experience is a mix of trust and availability. Organizations' brands take a hit if either factor falters. C-suite executives are keenly aware of the effect of security threats on business.

Events that influence changes in organizations security:

- 61% high-profile data breaches on peer companies
- 59% data breach or cyberattack with own organization
- 48% governmental regulations like GDPR, PCI, HIPAA, etc.
- 37% change in C-suite leadership

Balancing Investments and Risks

As the threat of network attacks becomes a question of 'when' and 'not if', organizations must carefully evaluate the risks associated with security vulnerabilities and the costs of implementing effective security solutions. At the same time, C-suite

executives face tough choices when deciding where to invest resources to propel their businesses forward.

Even though the threat of network attacks hangs over their organizations, about 25% of executives do not have or are in the planning stages of addressing key security concerns, such as performing security assessments on new technology or working with educational institutions to proactively recruit security specialists.

Most executives across regions (65%–81%) feel that their internal security resources are sufficient to handle their security needs. Yet 66% believe that hackers could penetrate their networks. The internal skills gap is not easily solved because the demand for security professionals outpaces the supply. As a result, more executives need to look to outside security vendors for assistance.

C-suite View of Current Network Threats – Key Findings:

- 66% had a hacker penetrate their network
- 54% experienced a data breach from one of its mobile applications in the last 18 months
- 57% had experienced a cyberattack in the last 12 months
- 50% were concerned about the security vulnerabilities created by use of multiple clouds

Impacting Vertical Industries

The impacts of attacks on corporate networks can vary depending on the industry in which companies compete. Security trends specific to the needs of some verticals:

Retail: In the retail sector, almost two-third organizations have a half of their business applications in the cloud and are concerned about security vulnerabilities between cloud networks. A major cause of concern for the executive suite is the fact that almost 20 attacks have happened in the past year. Data breach within their own organization was the most influential event that affected their own security planning. This can be troubling because they have the most customer touchpoints on their networks to enable e-commerce. Therefore this vertical definitely needs a security protection.

Manufacturing: Manufacturers have long embraced automation as a means to improve efficiencies and boost production. So it's not surprising that they focus on managing the increasing complexity of their IT infrastructures with plans to integrate automation (43%) to help automate security measures.

To accomplish this, about 75% of executives shared that they shifted more of the IT budget into security automation. Also, most keep tabs on what's happening in the marketplace, and two-thirds reported that high-profile data breaches at peer companies were the most influential event that affected their own security planning.

Finance: Corporate networks are the lifeblood of finance companies' businesses, which is why this vertical is likely to invest more in security to protect its assets. For example, Deloitte5, which suffered a cyberattack in 2017, said that it plans to spend 580 million USD on security over the next three years. These companies are especially aware of what's happening at peer companies. About 86% reported that high-profile data breaches at peer companies were the most influential event affecting their own security planning.

Looking forward, C-suite executives recognize the multiple pressures on their organizations to integrate new network technologies, transform their businesses and defend against cyberattacks, which are growing in frequency and complexity. As more companies add a mix of multiple public and private cloud environments to their IT architecture, the introduction of new vulnerabilities puts corporate and customer data at risk.

The stakes are high. Security threats can seriously impact a company's brand reputation, resulting in customer loss, reduced operational productivity and lawsuits, which reinforces that cybersecurity remains a priority in the minds of executives around the world. ■

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

Simplifying Multicloud Security With Managed Services

A managed security service provider can help CIOs and CISOs simplify their multicloud security environment, and help create a robust, sustainable and scalable security position for the enterprise

By Nitin Mishra

Enterprise IT has evolved dramatically over the last few years. Customer engagement and inter-connectivity are at the centre of every business application today, and cloud based applications have become the new normal. With more and more organizations now adopting multi cloud environments, security challenges have become even more complicated. While multi clouds offer unmatched flexibility in deployment and workload performance, they often lead to integration complexity, new security challenges and added vulnerabilities.

Managed security services can be a good way to tackle the challenges. A managed security service provider can be help CIOs and CISOs simplify their multicloud security environment, and help create a robust, sustainable and scalable security position for the enterprise. Here are three reasons why you need to partner with an established and state-of-the-art MSSP for multi-cloud security.

Handling Coverage and Complexity

With multicloud environments, security perimeters of IT organizations have widened far beyond their traditional scope of coverage. While allowing different business units operate on different cloud environments may bring home several cost and availability benefits, managing your IT security position in this dynamic environment is something that IT teams are not used to (or have been trained for).

For example, in a banking scenario, mobile apps today not just allow access to customer data but also provide the ability to perform a wide range of operations – such as banking transactions, mutual fund portfolio management, insurance purchases, loan applications, etc. Often, these workloads are placed in different clouds, and even different organizations. Across this environment, we can expect continuous changes to applications, data architectures and security protocols. The cloud vendors in use also keep adding new features and extending their platform capabilities, which further complicates the environment.

The MSSP Advantage: In such scenarios, managed security services can help organizations simplify and consolidate their security environment using a single layer (that includes security management, dashboards, people and standard processes). This has two important benefits: (a) scalability using a SaaS based model and (b) readiness to adapt and evolve the security environment to stay aligned to a continuously changing IT environment.

Addressing New Risks

Creating a loosely coupled cloud ecosystem also creates new risks. For example, there may be cases where teams make ad hoc or unannounced additions of shadow applications, or introduce new cloud platforms. In such scenarios, CIOs and CISOs need to rethink their IT security approaches and account for the added complexity that multicloud brings. Not to mention the added pressures of increasingly stringent regulations and security norms to protect data.

User demographics and motivations are also changing. More and more enterprise applications and data are being exposed to consumers, regulatory bodies, partners and other stakeholders. In the wake of a rapidly evolving user landscape, it is hard for security officers to overlook the ocean of possible threats such as uncharacteristic activities, untrusted modifications and unauthorized access.

> With the definition of enterprise IT environment continuing to change, the complexity of handling a multicloud scenario will keep on increasing

The MSSP Advantage: The pace at which such threats occur give organizations very little time to react address each and every change across all IT assets across the organization. Since the rate of obsolescence in the world of IT security is high, building this level of security preparedness would be extremely cost and resource intensive for individual organizations. MSSPs have the necessary scale to make continuous investments in skills and technology tools to monitor, detect and react to changing security needs.

Aligning Multiple Cloud Platforms

Although all major cloud vendors offer adequate security controls for the data and assets specific to their environments, they differ from each other in approaches to data back-up, access controls, compliance and other security features. As a result, data security officers are poorly positioned to develop a well-coordinated, unified response to any breach or attack. The problem amplifies when you have data being shared across different cloud providers, often making it difficult to meet overall compliance norms.

The MSSP Advantage: Finding a common ground to build a centralized orchestration across all your cloud platforms environments, and address the above challenges, becomes a key imperative. Without partnering with a proven MSSP, organizations may end up with a sub-optimal security position, and expose themselves to new, less understood risks.

With the definition of enterprise IT environment continuing to change, the complexity of handling a multicloud scenario will keep on increasing. Without a robust multicloud security approach, organizations risk growing overheads, skill shortages and new vulnerabilities. Therefore, irrespective of where they are in their multicloud journey, IT decision makers need to think well in advance about their security challenges and take proactive steps to mitigate risks in this new and fast changing environment. ■

The author is Senior Vice President & Chief Product Officer, Netmagic (An NTT Communications Company)

Can Alibaba Cloud Effectively Challenge The Big Three In India?

Alibaba has several challenges not the least of which is the skepticism about giving custody of your data to a Chinese company

By Shyamanuja Das

The recent launch of Alibaba Cloud's distribution channel and its announcement that it would train 1,000 sales and technology personnel in India in the next six months hit headlines in Indian media.

Alibaba chose a media conference that it held alongside its recent three-city partnership summit, called India Eco Summit, to make the announcement. The company's priority, said Dr Alex Li, General Manager for Alibaba Cloud APAC, are three: establishing its brand as a leading technology company, project itself as an expert in digital transformation and build a sustainable partnership ecosystem.

At this point, it is worthwhile to ask a basic question: how much chance does it stand in the wake of competition from the Big Three—Amazon Web Services (AWS), Microsoft, Google—and IBM, which are relatively well-entrenched in the market?

To be sure, Alibaba is no pushover. It is the fourth largest global player in public cloud infrastructure services, next only to the top three. In the most recent quarter (JFM 2018), it overtook IBM to take the No 4 spot globally.

While AWS led with a revenue of USD 5.44 billion, Alibaba Cloud registered USD 699 million revenue in the same quarter, behind Google's USD 1.2 billion, in the same quarter.

However, much of that is skewed because of its dominant market share (48%) in a big market, China. The Chinese market is so big that even the No 2 Tencent shows up in the top five list of APAC region.

In other regions, Alibaba Cloud is not even in top 5. However, of late, it has aggressively gone global with sponsoring the Olympics games for 12 years. That makes it the worldwide cloud service provider for both Summer and Winter Olympics.

The India Challenge

From the three priorities that Alibaba Cloud APAC GM Dr Alex Li identified, there was little specific on how it wants to build its brand as a leading technology company or drive the message of its positioning as "digital transformation expert". In the media conference too, questions regarding positioning of Alibaba Cloud among target customers, especially in comparison to the larger hyperscale providers, did not get too much specific information, whereas the channel plans were well elucidated. Market sources say all the marketing and communication plans of the company are now focused around the partners, not the users.

In essence, the first steps of Alibaba Cloud show that it is taking a channels-led approach and will go for push approach than big bang marketing to the users. A channel partner said the pricing may be 'aggressive' though he refused to comment beyond that.

From among the few specifics that Dr Li elaborated, one thing that stands out is the verticalized go-to-market approach that Alibaba will take. According to him, Alibaba Cloud will choose a few specific verticals initially and will try to build one or two good references before going all out for clients. This again is in synergy with the sales led approach, as compared to the marketing-led approach of the top three.

Of course, in a market like India, no cloud provider can afford to ignore the start-up ecosystem. IBM, Google, Microsoft and AWS have specific programs for this market. And, so has Alibaba Cloud.

"Alibaba Cloud will also build specialised teams to focus on various market segments and sectors such as start-up and online business, to provide customers with a single alignment to partners in order to promote business growth," the company said.

Being Chinese in India

But beyond the strategy and positioning as a cloud service provider, another thing that will be a major roadblock for Alibaba is the fact that it is a Chinese company.

While consumer products such as Chinese phones and applications like UC Browsers are popular in India, enterprises are a different market.

"Forget other strengths and weaknesses, will you like to host your data with a Chinese company," asked the CIO of a company in the broader travel industry, when this writer quizzed him on the possible impact of Alibaba Cloud's entry in the Indian market. That was the end of discussion.

This is a very real challenge for the company. It is one thing to talk about your offering, support, availability of services, differentiation, pricing...it is another thing to fight the perception about your origin and nationality. In India, the mind block against giving your data to a Chinese company.

Beyond the usual suspicion, in the Indian government circles, there is suspicion about the Chinese. Last year, media reported, in the wake of border standoff, the Indian government went for testing the popular Chinese mobile bowser, UC Browser to verify if it was leaking data. Incidentally, UCWeb, the maker of the browser is a subsidiary of Alibaba Group Holding.

Going for a Chinese company to host your application or data, is one level of extra challenge for Indian companies that they have to take if they do not want to get on the wrong side of the government.

It is naïve to believe that Alibaba Cloud is not aware of this. Probably that has made it approach the hyper price sensitive segment of small enterprises first.

To address localization needs, it has already set up its first data center in Mumbai.

Alibaba Cloud now has 47 availability zones across 18 economic centers globally, with coverage extending across mainland China, Hong Kong, Singapore, Japan, Australia, the Middle East, Europe, India and the U.S. (East and West Coast).

It is too early to take a call on Alibaba Cloud's chance in India. The company is yet to prove itself outside China. But in India, its challenge is even bigger. It needs to build a narrative that is not just differentiated from the top three but also convincing enough to dispel the doubts about a Chinese firm handling an Indian company's data. ■

How Likely Are You To Be Hacked?

F5 research reveals web and applications attacks are the largest cause of security breaches

Data breaches continue to be a threat to enterprises and consumers. In 2016, 3.2 million credit card and debit card details were stolen by Chinese hackers. The Food and Civil Supplies Department of Chandigarh had reportedly published Aadhaar numbers of their public distribution system beneficiaries in April last year. A couple and one month later, the Jharkhand Directorate of Social Security had reported a similar leak.

And since data is gold, applications are increasingly the target of cybercriminals. New research by F5 Labs found that web and applications attacks are the largest cause of security breaches (30%), with an average reported cost of close to USD 8 million per breach. It also found that a typical organization runs 765 web applications, with 34% of them considered mission-critical.

The research, using data gathered from Loryka and WhiteHat Security, provides analysis of the current threat landscape, detailed research stats and steps to secure applications to protect users and data.

Highlights from the F5 Labs' *Protecting Applications 2018 Report* include:

Denial-of-service (DDoS) Attacks

- Credential theft, DDoS attacks, and web fraud are the top three attacks that are the most devastating to organizations represented in the global study.
- 69% of respondents in China and India are most concerned about DDoS attacks.
- APAC accounted for 17% of DDoS attacks in 2017, with a spike from Q4 2017 to Q1 2018.
- Security Response: DDoS attacks are pervasive across all levels of the application tier. It is critical that every organization has a DDoS response strategy.

Account Access Hijacking

- Breach records analysis shows that 13% of all web app breaches in 2017 and 1Q 2018 were access-related.
- Some of the top categories were:
  1. Credentials stolen via compromised email (34%)
  2. Access control misconfiguration (23%)
  3. Brute force attacks to crack passwords (5%)
  4. Credential stuffing from stolen passwords (9%)
  5. Social engineering theft (3%)
- Security Response: Stronger authentication solutions for mission-critical applications or for external applications over which organizations don't have full control.

Injection Attacks

- Injection attacks allow an attacker to insert commands or new code directly into a running application with malicious intent.
- Injection vulnerabilities (weaknesses that have not yet been exploited) are prevalent. Those composed 17% of all discovered vulnerabilities in 2017.
- Security response: High priority should be given to finding, patching, and blocking injection vulnerabilities.

Opportunist attackers keep their ROI high by keeping costs low… They come at you with canned exploits and known methods. If rebuffed, they quickly move on to the next target

How likely are you to be hacked?

In general, there are two types of attackers: Opportunists and targeted attackers:

- **Opportunist attackers** keep their ROI high by keeping costs low. They use a spray-and-pray approach to sweep the Internet looking for easy pickings. These attackers come at you with canned exploits and known methods. If rebuffed, they quickly move on to the next target.
- **Targeted attackers** choose their targets carefully. Their goal could be espionage or a high payoff, but it's likely that once you're in their sights, they're coming after you. Though less prevalent, such attackers are generally more motivated.

How can organizations improve application security?

Below are four low-difficulty steps:

1. **Understand your environment:** Know what applications you have and what data repositories they access.
2. **Reduce your attack surface:** Attackers will probe any part of an application service that is visible on the internet for possible exploitation.
3. **Prioritize defenses based on risk:** Know which applications are important and minimize the attack surface by identifying applications that need additional resources.
4. **Select flexible and integrated defense tools:** Have a good but manageable selection of flexible, powerful solutions to cover controls for prevention, detection, and recovery from existing and emerging threats.

Building a solid application defense strategy requires understanding each app and its areas of vulnerability, assigning an appropriate level of risk to the app according to the value of the data it contains, and taking a holistic view to securing applications based on their vulnerabilities, threats, and level of risk. ■

Is Your Data Hack-Proof?

As organizations struggle to maintain and protect their customers' data, there is a growing concern amongst their customers about the security of their personal information

By Ved Prakash

Just when the global cyber community was slowly recovering from the infamous WannaCry Ransomware attacks that caused havoc across the globe last year, two recent cyberattacks of an almost identical nature again shook the cyber community worldwide.

In May 2018, two Canadian banks, The Bank of Montreal and CIBC-owned Simplii Financial, were targeted by hackers who managed to get access to the personal information of thousands of their customers. The hackers demanded a ransom of USD 1 million from each bank failing which they threatened to publish the stolen information on the internet. The information that the hackers got access to included the names, dates of birth, social insurance number, debit card details, home address, occupation, marital status, secret questions and account balances. Security experts suspect that the hackers used a 'spear phishing' attack in which they targeted specific people who had accounts with both these banks and used malicious cyber techniques to make them hand over their crucial data.

Why did this Happen?

Organizations, especially banks, store a lot of user data to help them service their customers, target marketing activities and run analytics to make their products/services relevant to the needs and demands of the market. Broadly, user data can be classified into two types: Personally Identifiable Information (PII) and Non-PII. In simple words, any data that can be used to identify the identity of a person is categorized as PII. This leads to an inherent need of storing and managing PII in a more secure manner as compared to the non-PII data.

In the case of Bank of Montreal and Simplii Financial, the breach happened despite both the banks having implemented stringent perimeter security controls. Cyber security experts feel that had the banks employed data encryption technologies for securing their customers' PII stored within their database, then such an attack would not have been possible.

While there are many encryption alternatives available in the market today, most businesses find themselves lacking when it comes to management of the encryption keys

The Way Forward

Hackers have been around since the time the Internet was born and with every passing day, their numbers are increasing manifold with data breaches taking place almost on a daily basis. According to Gemalto's *2017 Breach Level Index Report*, the number of data records compromised in publicly disclosed data breaches surpassed 2.5 billion – a whopping 88% from 2016. This equates to more than 7 million records lost or stolen every day, or 82 every second!

With rising incidents of data breaches, the business impact goes way beyond a financial hit. As organizations struggle to maintain and protect their customers' data, there is a growing concern amongst their customers about the security of their personal information. Gemalto's recent *Customer Loyalty Survey* interviewed 10,000 consumers worldwide revealed that a majority (70%) of consumers would stop doing business with a company if it experienced a data breach.

This figure alone should ring the alarm bells of organizations that store their customers' PII without deploying robust data encryption technologies. Encryption involves scrambling of the data using an algorithm with a key to create a code – the encryption key. Unless a user has access to the key, the data cannot be unscrambled or decrypted.

However, securing the data does not end with merely encrypting it. Encryption transfers the responsibility of enterprise security from the data to encryption key management – a holistic solution that is seamlessly able to generate the encryption keys, distribute, rotate and store them and revoke/destroy the keys, as needed. In a nutshell, businesses need an end-to-end data encryption solution to ensure the security of data.

While there are many encryption alternatives available in the market today, most businesses find themselves lacking when it comes to management of the encryption keys. It's like putting a lock on all the doors of your room and not knowing where the keys are. This can still lead to a potential theft if the keys land in the wrong hands. Hence, having a centralized platform that can help organizations manage their crypto keys across all stages of their lifecycle can play an important role in ensuring optimal data protection.

What's needed is a robust and centralized key management solution that can be seamlessly deployed in physical, virtual, and cloud environments. Some of the salient features that play a crucial role in data security are:

1. Heterogeneous key management – helps in managing multiple crypto keys for different types of encryption products.
2. Multiple use cases – easily integrates with other data protection solutions.
3. End-to-end key-lifecycle support
4. Centralized management console – helps in assigning administrator roles according to the scope of their responsibilities.
5. Logging and auditing – helps in storing audit trails that can be analyzed by using any leading SIEM tools.
6. Reduces the overall cost of data security by offering automated operations.

To Sum It Up

What would you do if an organization didn't take the security of your data seriously? Probably stop using their products/services, right? Most of us would do the same. We are all concerned about the security and privacy of our data gathered by various businesses. As consumers, we expect all organizations, no matter how big or small, to employ the latest security tools.

When we look at it from the other side of the line, as business owners, we tend to try and get by with the security system already in place. However, hackers are evolving and your data security tools need to keep up too. An end-to-end data encryption solution can ensure that you and your customers can be assured of maximum data protection. Remember, if your customers feel that your organization places security of their personal information at the top of the priority list, he/she would not just be loyal to your brand but also work as a powerful brand ambassador. ■

The author is Senior Business Development Manager – Banking Identity & Data Protection Enterprise & Cyber security at Gemalto

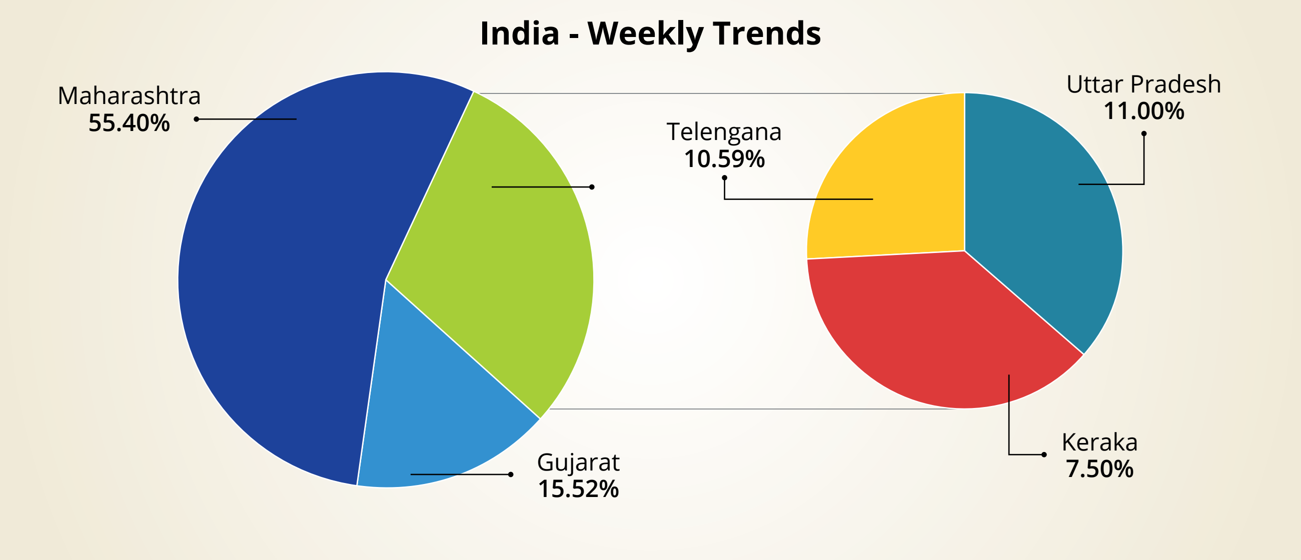
Now A New Wave Of Ransomware In India?

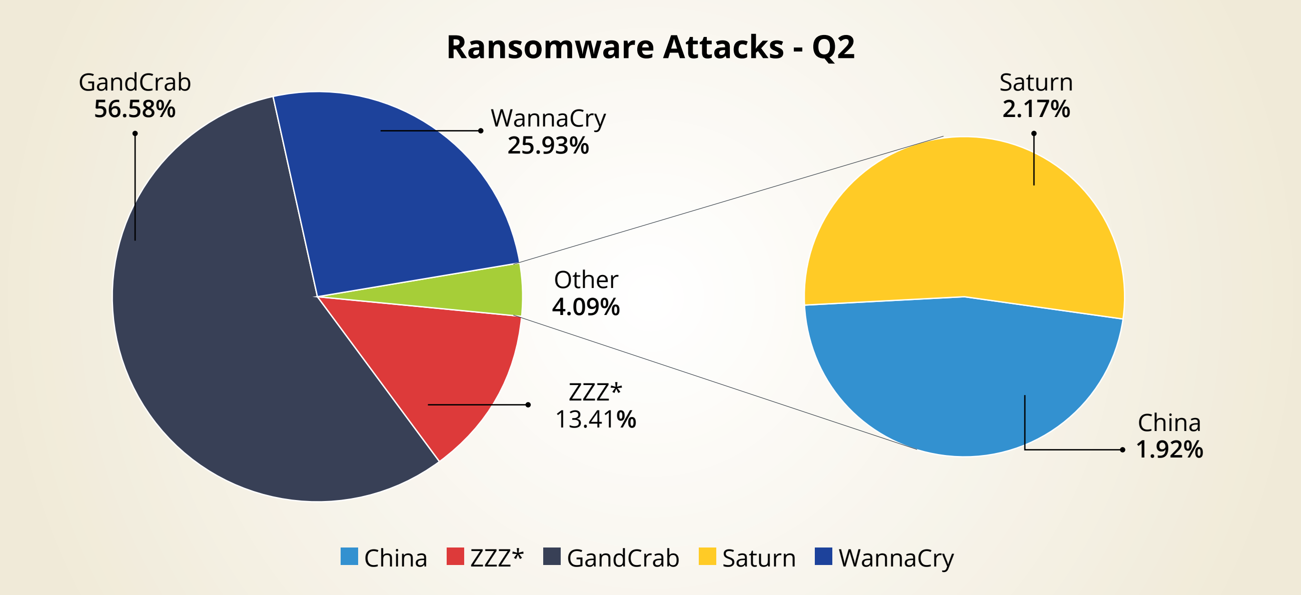
eScan reveals presence of various variants and newer Ransomware in India besides existence of WannaCry in dormant form

Last year WannaCry created havoc across the globe and due to its lateral movement; it had penetrated into the networks and skipped across the countries and continents. The security community has been highly proactive in taking down the infrastructure associated with WannaCry, however, eScan observes that due to its ability to move across networks, it still exists in its dormant form.

eScan's telemetry servers have been picking up reminiscent artefacts of WannaCry Ransomware on a regular basis. Over the period of past few months, we have observed a steady decrease of incidents involving WannaCry and hopefully by the year end WannaCry should meet the same fate as that of Conflicker Worm/DNS Changer Botnet.

eScan has further observed various variants and newer Ransomware being added into the family. However, very few have seen active development, viz., GandCrab and ZZZ*. In last few weeks, GandCrab has taken the center-stage and is evolving at a much faster rate, which suggests that the Ransomware Developer/Criminal nexus is growing stronger





and many of the criminals are now switching their loyalties to GandCrab due to the sheer fact that the developers are taking keen interest and adding numerous weapons to its arsenal.

The next step of evolution for Ransomware would be cryptominers with info stealers and a Ransomware all bundled into one.

India has seen its share of Ransomware attacks and Maharashtra leading the way for the week, however, in states like Gujarat, Telengana, Uttar Pradesh and Kerala we have observed a rise in activity of the GandCrab Ransomware Attacks while xtbl, korean, Dharma and CrySiS variants of Ransomware family are still making rounds.

Prevention Measures:

- To stay safe from such ransomware attacks, all the organizations and users need to ensure that, the patches released by Microsoft have been updated or patched immediately.
- Administrators should block all executable files from being transmitted via emails.
- Administrators should isolate the affected system in the network.
- Administrator can restore the encrypted files from the backup or from system restore point (if enabled) for affected systems.
- Install and configure eScan with all security modules active:
  1. eScan real-time monitoring
  2. eScan proactive protection
  3. eScan firewall IDS/IPS intrusion prevention
- Users shouldn't enable macros in documents.
- Organizations should deploy and maintain a backup solution.
- Most important, organizations should implement MailScan at the gateway level for mail servers, to contain the spread of suspicious attachments. ■

Global Spending On Robots And Drones To Grow Rapidly Over The Next Five Years: IDC

The global spending will reach USD 201.3 billion in 2022 and achieve a compound annual growth rate (CAGR) of 19.6% over the 2017–2022 forecast period

Global spending on robotics and drones solutions will reach USD 201.3 billion in 2022 and achieve a compound annual growth rate (CAGR) of 19.6% over the 2017-2022 forecast period, according to IDC's Worldwide Semiannual Robotics and Drones Spending Guide. Robotics and drone spending will reach USD 95.9 billion in 2018.

Spending on robotics solutions will total USD 86.6 billion in 2018 and will account for more than 85% of all spending throughout the five-year forecast. Industrial robotic solutions will account for the largest share of robotics spending (more than 57%), followed by service robots and consumer robots. Discrete and process manufacturing will be the leading industries for robotics spending at more than USD 54 billion combined in 2018. The resource and healthcare industries will also make significant investments in robotics solutions this year. The retail and wholesale industries will see the fastest robotics spending growth over the forecast with CAGRs of 32.7% and 30.7%, respectively.

"Collaborative robots are taking off in industrial applications, driven by customer demands for product quality, delivery, and mass customization," said Dr. Jing Bing Zhang, research director, Worldwide Robotics. "While being safe is the prerequisite for any collaborative robot, the market is already shaping the development of collaborative robots towards simplicity, smartness, and ease of redeployment."

Worldwide drone spending will be USD 9.3 billion in 2018 and is expected to grow at a faster rate than the overall market with a five-year CAGR of 32.1%. Enterprise drone solutions will deliver more than half of all drone spending throughout the forecast period with the balance coming from consumer drone solutions. Enterprise drones will increase its share of overall spending with a five-year CAGR of 37.1%. The utilities and construction industries will see the largest drone spending in 2018 (USD 925 million and USD 808 million, respectively), followed by the process and discrete manufacturing industries. Key growth in drone spending will come from various industries including education (72.8% CAGR) and federal/central government (70.1% CAGR).

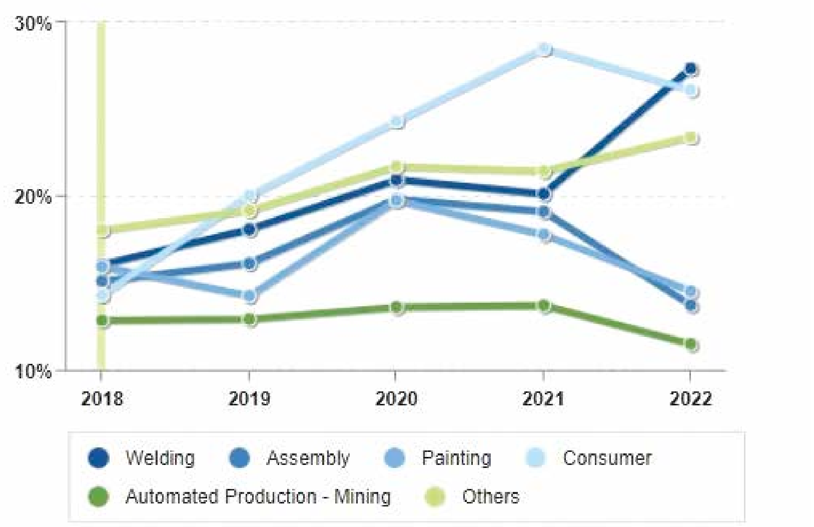
"Organizations continue to explore a range of applications and use cases for drones, moving beyond aerial photography to drone-based deliveries, precision agriculture monitoring, and even time-sensitive medical deliveries. With these expanded use cases come concerns across many governing parties. Most regions, however, are starting to provide regulatory clarity, as they understand the growing need for drone control and an air traffic management system for both enterprise and consumer deployments. In addition, as safety continues to be a major concern for consumers and regulators, vendors and IT suppliers are working to alleviate concerns by building drones with multiple redundancies, improving their sensory and collision avoidance technology, and testing 5G-enabled drones to enable greater connectivity while lowering latency. The sky's the limit," said Stacey Soohoo, research manager, IDC's Customer Insights & Analysis.

The use cases that will capture the largest share of robotics and drones spending are driven by their respective industries. As the primary use case in the Discrete Manufacturing industry for robotics, welding is forecast to receive over 15% of all robotics spending worldwide throughout the forecast. Other robotics use cases that will drive spending include assembly, painting, mixing, automated production in mining, and pick and pack. The use cases that will see the fastest growth in robotics spending over the forecast period include break bulk (53.4% CAGR), shelf stocking (45.6% CAGR), and customer service (42.0% CAGR). For drones, the use cases that will see the fastest growth over the forecast period include dispensing pesticides and fertilizer (109.4% CAGR), emergency service (86.4% CAGR) and precision agriculture/crop scouting (86.1% CAGR).

More than half of all robotics spending this year (USD 58.1 billion) and throughout the forecast will go to robotics systems, after-market robotics hardware, and systems hardware. Services-related spending, which encompasses application management, education & training, hardware deployment and support, systems integration, and others will total more than USD 16.7 billion in 2018 while spending on command and control, specific robotics applications, and network infrastructure software will reach USD 11.8 billion. Purchases of drones and after-market drone hardware will be nearly USD 7.9 billion in 2018 while spending on command and control, specific drone applications, and network infrastructure software will reach USD 611 million.

On a geographic basis, China will be the largest geographic market for robotics, delivering more than 30% of all robotics spending throughout the forecast, followed by the rest of Asia/Pacific (excluding China and Japan), the United States, and Japan. The United States will be the largest geographic market for drone spending at USD 4.3 billion in 2018, followed by Western Europe and China. However, exceptionally strong spending growth in China (63.2% CAGR) will move this market ahead of the United States by 2022. ■

Top Use Case Based on Spend, 2018: Annual Growth (%) (Value(Constant Annual))



Source: IDC Worldwide Semiannual Robotics and Drones Spending Guide, 2017H2

The Switchover To Services Is Finally Happening In Security

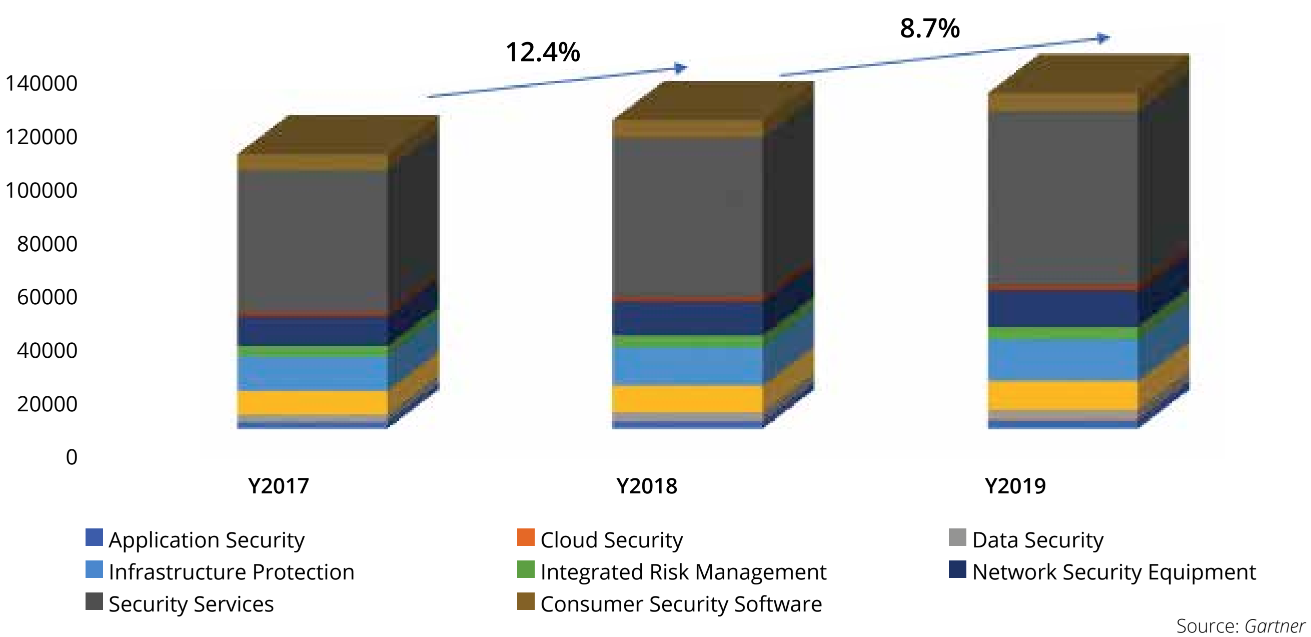
A Gartner forecast says despite significant growth, cloud security will remain a small fraction of the overall market

Security services now account for more than half of the overall security spending in the enterprise and will remain that way for the next two years, according to data on worldwide spending on information security, released by Gartner.

Garter says overall security spending will grow by 22% between last year and 2019 and will reach USD 124 billion in that year, up from USD 101 billion last year. The research firm says this year the spending will be USD 114 billion.

While security services would account for 52% of the total security spending, traditional segments like infrastructure security and network security will account for 12% and 11% respectively. The spending mix is not likely to change much between 2017 and 2019, despite a significant rise in spend in cloud security, which still accounts for a very small fraction of the overall security spend.

Between 2017 and 2019, spending on cloud security will more than double to USD 459 million while data security too will register a significant growth, recording a growth of 37% from between last year and 2019. Most other enterprise security segments will grow around 20-25%, Worldwide Security Spending Growth Forecast



Source: *Gartner*

according to Gartner forecast.

"Security leaders are striving to help their organizations securely use technology platforms to become more competitive and drive growth for the business," says Siddharth Deshpande, research director at Gartner. "Persisting skills shortages and regulatory changes like the EU's Global Data Protection Regulation (GDPR) are driving continued growth in the security services market."

A 2017 Gartner survey had revealed that the top three drivers for security spending are: (1) security risks; (2) business needs; and (3) industry changes. Privacy concerns are also becoming a key factor.

"Privacy concerns will drive at least 10% of market demand for security services through 2019 and will impact a variety of segments, such as identity and access management (IAM), identity governance and administration (IGA) and data loss prevention (DLP)," the company says.

'Highly publicized data breaches, like the recent attack on SingHealth that compromised the personal health records of 1.5 million patients in Singapore, reinforce the need to view sensitive data and IT systems as critical infrastructure," says Deshpande.

An increased focus on building detection and response capabilities, privacy regulations such as GDPR, and the need to address digital business risks are the main drivers for global security spending through 2019.

Key Trends

Some of the key trends identified by the research firms are:

- At least 30% of organizations will spend on GDPR-related consulting and implementation services through 2019. Organizations are continuing their journey toward compliance with the GDPR that has been in effect since 25 May 2018. Implementing, assessing and auditing the business processes related to the GDPR are expected to be the core focus of security service spending for EU-based organizations, and for those whose customers and employees reside there.
- Risk management and privacy concerns within digital transformation initiatives will drive additional security service spending through 2020 for more than 40% of organizations. Consulting and implementation service providers have retooled their service offerings over the past several years to support customers on their digital transformation journey. Security is a key factor in the uptake of that transformation process for regulated data, critical operations and intellectual property protection spanning public cloud, SaaS and the use of Internet of Things (IoT) devices.
- Services (subscription and managed) will represent at least 50% of security software delivery by 2020. Security as a service is on the way to surpassing on-premises deployments, and hybrid deployments are enticing buyers. A large portion of respondents to Gartner's security buying behavior survey said they plan to deploy specific security technologies, such as security information and event management (SIEM), in a hybrid deployment model in the next two years. Managed services represented roughly 24% of deployments, on average■

CFO INDIA NETWORK

Intelligence . Leadership . Transformation

A PEER-POWERED,
KNOWLEDGE - BASED AND
COMMUNITY-LED INITIATIVE
FOR CFOs

#TheBigPicture

42% of the winners report to a C level

64% of winners work in organizations with IT budget of over 10 crore and above

Come and establish camaraderie with the IT giants of tomorrow

INDIA's FUTURE CIOs
NEXT100
2018

For engagement opportunities, please contact

Mahantesh G	9880436623	mahantesh.g@9dot9.in
Deepak Sharma	9811791110	deepak.sharma@9dot9.in
Prashant Amin	9820575282	prashant.amin@9dot9.in
BN Raghavendra	98453 81683	bn.raghavendra@9dot9.in
Vandana Chauhan	9958984581	vandana.chauhan@9dot9.in

Apply for the NEXT100 today—it could change your life. Go to: www.next100.in

Why Cisco Has Fallen In Love With Networking All Over Again?

By helping it show a direct linkage between business logic and physical networks, Cisco's intent-based networking helps the company project a more evolved meaning of networking

By Shyamanuja Das

Recently, Cisco shares dropped 3% in a day on reports that Amazon (AWS) was considering entering the networking switches market, which Cisco has dominated for long. It bounced back only when financial information site, Marketwatch quoted a Cisco spokesperson that AWS CEO Andy Jassy had clarified to Cisco CEO Chuck Robbins that the former was not building a 'commercial' switch.

The impact of the news on Cisco's stock price is an indication of how much investors see Cisco as a 'networking' company, even though Cisco has come a long way from the days of routers and switches only company.

Cisco is now a market leader in unified communication, security and cloud infrastructure market. But for some reason, Cisco was defensive talking about its infrastructure. Maybe, it did not have a nice 'story' to tell how its components were all part of an offering that provided greater value than the sum of parts.

This was as late as in 2017. At least, that was the conclusion after one attended its 2017 India media briefing at Manesar near Delhi. Why else would a company black out one big piece of its business where it was the dominant market leader? The two days focused on collaboration and security—so much so that half of the event was dedicated to security. As we wrote in a report then, cloud story was missing almost entirely.

One can only guess if it was dictated by local/logistic consideration or if there was a bigger reason behind it. But if it was the latter, it was surely not there this time around—the 2018 media conference at Goa.

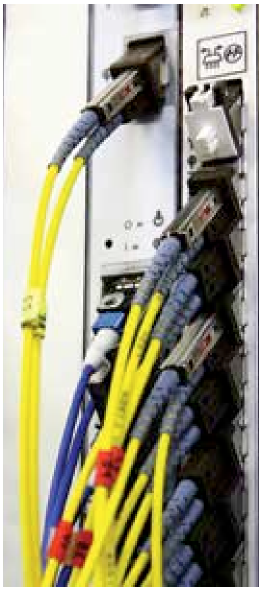
This is why we say so.

First of all, the coverage was much wider. Security, Collaboration, Cloud, Service Providers, Transformation, Services, and yes Networking—each of these were covered by respective business leaders.

Second, there was a holistic story that tried to show how each of the pieces joined together. While the business leaders focused on their pieces, CIO V C Gopalarathnam focused on future and India president Samir Garde focused on India plans as well as the five areas in which Cisco could help its components. They were:

- Reinvent the network
- Security is foundational
- Unlock the power of data
- Embrace the multi-cloud world
- Employee and Customer experience
- He applied each of these to India as a whole and outlined Cisco's India strategy.

But the biggest statement that came in the entire conference was Garde's proclamation—Cisco has fallen in love with networking again.



But the biggest statement that came in the entire conference was Garde's proclamation—Cisco has fallen in love with networking again...this was surely a change of heart, at the bare minimum.

The sentence said a lot.

For a company that was defensive talking about its oldest and biggest business, this was surely a change of heart, at the bare minimum.

What is behind this change?

Arguably, a better articulated positioning on its new management capability. It is not that the capability came to Cisco yesterday. But with the launch of its Digital Network Architecture (DNA) and its control software DNA Center, the proposition is far better pronounced.

Last year, during Cisco media conference, it had just been launched and was not part of its story, let alone being the centerpiece of its new networking proposition.

DNA Center helps businesses by automating a lot of management. What it means is that they don't have to rely on time-consuming human-powered workflows, making changes one network device at a time; they can interact with the network as a single fabric. And second, in case of an attack, the network can react to it in real time. Why, even provisioning can be automated on a real-time basis through policy setting. Cisco calls it intent-based networking because applications, services, and users are prioritized based on business intent.

India shows the way

While it is early days yet and the customer intent regarding deploying intent based networking is yet to be clear, India is seeing a lot of interest.

"India's response to intent-based networking has been phenomenal," says Rajesh Shetty, Managing Director, Enterprise Sales at Cisco India.

The reason is not difficult to understand. India has a huge base of IT/BPO services companies that operate large offshore dedicated centers for many of their clients. This means the segmentation is far easier. So, there's a lot of interest from those companies.

TCS, incidentally, is the largest customer of intent-based networking of Cisco globally.

Some of the other use cases could be in businesses where regulators influence a clear segmentation because of their mandate to have 'arm's length' relationships.

Intent-based networking is Cisco's proposition of closing the gap between physical networks and business logic. That probably explains Cisco's falling in love with networking again!

And India could give a whole new meaning to that romance! ■

Double Scoop

Two times
the revelation

CM Mohan Kumar

Director - Systems
VIT University

MY FAVOURITE SPORT

Cricket

A TECH EVENT WHICH I ATTENDED RECENTLY

VMware vForum 2018

AN APP WHICH I USE THE MOST

WhatsApp

MY FAVORITE SINGER

Dr. KJ Yesudas

MY TECH IDOL

Dr. APJ Abdul Kalam

MY PEER IN THE IT COMMUNITY

Sreevalsan Moothedath

Head – ICTS, Amrita University

MY FAVORITE SONG

Rim Jhim Gire Sawan

MY FAVORITE DRESS

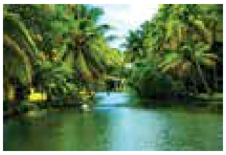
Kurta & Dhoti

A TECH SHOW WHICH I WATCH THE MOST

NDTV Gadgets

MY FAVORITE HOLIDAY SPOT

Kerala



THE SOCIAL MEDIA TOOL WHICH I MOSTLY PREFER

LinkedIn

डिजिट

अब हिंदी में

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

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

डिजिट