AISS 2013 RECOMMENDATIONS:
ADVANCING TOWARDS A SECURER CYBERSPACE
Data Security Council Of India (DSCI) is a focal body on data protection in India, set-up as an independent Self Regulatory organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same. DSCI is engaged with the Indian IT-BPM industry, their clients worldwide, banking and telecom sectors, industry associations, data protection authorities and other government agencies in different countries. It conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cyber crimes in the country and towards this; it operates several cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.

Public Advocacy, Thought Leadership, Awareness and Outreach and Capacity Building are the key words with which DSCI continues to promote and enhance trust in India as a secure global sourcing hub, and promotes data protection in the country.

For more details about DSCI or this publication,

Please contact:
+91-11-26155070/71 or write to us at media@dsci.in
It gives me great pleasure to present this report “AISS 2013 Recommendations: Advancing Towards a Securer Cyberspace”, which in essence is the outcome of the NASSCOM-DSCI Annual Information Security Summit 2013, held at the Grand, New Delhi on December 10-12. This eight edition of the summit attracted over 500 participants from over 250 organizations including government, law enforcement, defense, public sector, IT-BPM, banking, telecom, health care, manufacturing, insurance, energy, service providers, academia and others. Over 40 security vendors and services providers from around the world participated as sponsors and exhibitors and provided insights into the latest technology trends and demonstrated innovative products.

It was our privilege and pleasure to have Shri Kapil Sibal, Hon’ble Minister of Communications & IT, inaugurate the Summit this year. In his inaugural speech, Shri Sibal encouraged the industry to strengthen cyber security and made a forceful case for India to become an active player in the areas of cyber security, Internet Governance, privacy, cloud computing, global standards, among other areas. He complimented NASSCOM and DSCI for organizing a very well researched Summit and increasing awareness amongst stakeholders on a wide range of issues.

This report is an amalgamation of the ideas and thoughts of over 100 thought leaders and experts from diverse backgrounds and areas of expertise, and actionable insights from stakeholders. It incorporates inputs and suggestions from the multiple sessions of the Summit along with the key recommendations that emerged during the discussions.

I hope the policy makers, businesses, experts, delegates and sponsors will find this report relevant and valuable, and it will contribute in devising solutions to the issues and challenges we face in cyber security and data protection.

Dr. Kamlesh Bajaj  
CEO, DSCI
The NASSCOM-DSCI Annual Information Security Summit (AISS) is one of the flagship conferences of Data Security Council of India (DSCI) on information security in India. AISS started in 2006 to help drive the Information security agenda and induce related dialogues within the country. Through the history, the summit has consistently gathered all the relevant stakeholders including government, law enforcement, defense, industry, public sector, service providers, others and facilitated deliberations on contemporary issues and solutions making it a place where India meets for security.

AISS 2013 was the eight edition, held from December 10-12, 2013. The multi-day event agenda covered the contemporary trends and evolutions in cyber security and privacy through various means including workshops, technology insights, keynote sessions, plenaries, debates, policy deliberations and views of industry verticals. This year the summit expanded its scope, scale, offerings and opportunities with a special focus on:

- National Security
- Architectural Paths
- Policy Governed Systems
- Critical Internet Resources
- Criminal Networks
- Cyber Warfare
- Big Data
- Pre-emptive Striking
- Clean Pipe
- Operational Technologies
- Development and Operations (DevOps)
- Trust Overlay
- SIEM
- Cyberwar Mercenaries
- Privacy in global surveillance
- and much more.

100+ speakers, 40+ sessions, plenaries, multiple parallel track sessions, roundtables, breakfast meets and 10 keynote sessions.
DSCI Excellence Awards, which was instituted in 2011, to raise the level of security and privacy in the industry & awarding law enforcement agencies and officers for developing capacity in cybercrime investigation and solving cybercrime cases respectively, formed an integral part of the summit. Winners of DSCI Excellence Awards 2013 were felicitated by Shri G K Pillai, former Union Home Secretary, GoI in the Awards ceremony on December 11, in New Delhi.

DSCI Excellence Awards, in its third edition, included the below categories:

Corporate segment: DSCI Excellence Awards for Security in Bank, Telecom, e-Governance, e-Commerce, IT Services-Large & SME, BPM-Large & SME. Other Award categories include DSCI Excellence Award for Privacy, Information Security Product Company, Security Leader of the Year and Privacy Leader of the Year.

Law enforcement segment: India Cyber Cop of the Year and Excellence in Capacity Building of Law Enforcement Agencies

More detail covered at page [40-41]
KEY RECOMMENDATIONS

PRIVACY AND SECURITY CHALLENGES IN CLOUD COMPUTING

To establish a trusted and conducive global environment for cloud adoption, there is a need to bring in transparency in government surveillance and interception procedures, (may be through development of global norms for conducting surveillance), harmonize governments’ policies, laws and regulations that directly or indirectly regulate cloud services, and advance international, multi-lateral and bi-lateral agreements to promote cross border data flows. At a tactical level, model cloud contract should be developed to facilitate contract negotiations, cloud service provider certifications should be promoted to enhance assurance and very importantly the cloud service providers should provide timely support to the law enforcement agencies of different countries in crime investigations, and respect the law of the land. Finally, an institutional mechanism based on public private partnership (P-P-P) should be created to build trust and maturity in cloud computing.

INTERNET GOVERNANCE

While the ICANN tries to establish itself as a neutral independent international non-governmental body, global norms needs to be codified for Internet governance which provide directions and guidance for nation states to act, else the sovereignty issues will remain unaddressed. Any such global norm must recognize the role of different stakeholders including the private sector, technical communities, academia and civil society by making multi-stakeholderism the underlying principle. In doing so, defining ‘multi-stakeholderism’ and how it works is extremely important. The body responsible to manage Internet resources, whether ICANN or any new entity created, should be subject to International law and overseen by an international appellate, comprising of experts sponsored by respective governments. The global solutions that may emerge should strive to create necessary balance in cyberspace between freedom of expression and restrictions, national security and privacy, among others with the ultimate objective of welfare of the mankind. On the other hand, in establishing sovereignty, nations must not create hurdles for economy by demanding localization of ICT infrastructure, restricting trans-border data flows, among others.

India should deliberate the issue of governing cyberspace more comprehensively and increase participation and representation in global bodies, committees and forums to voice local concerns in a better fashion. The brainstorming should start within the government with inter-ministerial consultations and consultations with industry, civil society and academia should take place on a continuous basis. This will help in formulating India’s position in international discussions and negotiations regarding governance of cyberspace. More conferences, workshops and seminars on this issue should be held to raise awareness and outreach among the masses.
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Global security community needs to realize the cyber threat posed to critical information infrastructure (CII) connected to the cyberspace through the Internet or otherwise. To secure CII effectively there is need to develop, share, implement and audit security best practices with respect to controlling and monitoring of cyber physical systems. Further there is a need to continuously conduct critical examination of how the operational technologies work, how these technologies are evolving and marrying with the Internet technologies, and how they have been deployed for strengthening the CII cyber ecosystem. Last but not the least the global community should work towards developing international agreements, norms or resolutions to avoid cyber conflicts that involve disruption of CII through cyber attacks.

ROLE OF TELECOM NETWORK IN STRENGTHENING CYBER SECURITY

The governments and the telecom industry should collaborate at the national and international levels to strengthen cyber security. Government should empower the authorized agencies with necessary authority to take legitimate actions on the telecom networks to curb illegitimate activities such as running of bot networks. Specifically with respect to botnets, education and awareness to end users is of utmost importance as they form the source of compromised systems. Leveraging technology solutions, the traffic should be screened at the gateway level based on well-defined rules to identify and terminate the malicious content. Appropriate privacy protection safeguards should be designed and integrated in the operationalization of such a screening system. To enhance security of telecom networks and cyber security in general, telecom equipment and systems should be designed and tested based on globally accepted standards.

PRIVACY IN THE AGE OF DATA ANALYTICS

The advanced methods and capability to mine personal data and analyze it for actionable intelligence are available with governments and organizations today. While this data may be used to benefit nations and communities, it is imperative that a legal framework is available to ensure governance of data with respect to privacy. The legal framework should not unnecessarily create legal or administrative hurdles in the name of privacy protection; instead it should recognize the economic value of data and promote data flows. The parties responsible for collection of data should be made responsible and held accountable for the personal information they possess, process or part- with. Implementation of user-centric privacy principles such as notice, choice and consent need to be made more meaningful and
transparent. Organizational centric privacy principles such as collection limitation and use limitation need to be imbibed in the DNA of organizations. Given that the subject of privacy requires greater research due to its wide-reaching impact on the socio-political structure of a nation, policy research institutions or centers, under the P-P-P model, should be established in India to provide guidance on matters related to national security, public order, disclosure in public interest, protection of the individual and industry specific practices and standards for safeguarding personal information.

**DIGITAL FORENSICS IN SOCIAL, CLOUD & MOBILE ENVIRONMENT**

The law enforcement agencies (LEAs) are facing issues in getting lawful access to data stored in the cloud (which is located outside their country) for the collection of evidence in criminal investigation. The cloud services providers should respect the local laws of the countries, irrespective of the geographic location of ICT equipment and timely share the data with the LEAs under the legal process. In this regard, a Service Level Agreement (SLA) with the service providers should be signed and enforced. Technological and operational capabilities need to be developed, which can be deployed by the cloud service providers to maintain the data in a format that is readily usable by the LEAs. The chain of custody of digital evidence should be maintained. To strengthen international cooperation, India should carefully review the pros and cons of the Budapest Convention on Cyber Crime and decide on signing the agreement.

**CYBER WARFARE**

A global agreement or arrangement should be made to classify defensive and offensive cyber technologies and control the development and usage of cyber offensive technologies by nation states. India should also develop a cyber warfare doctrine in which it should define the threshold till which the impact of cyber-attack can be tolerated without retaliation. There needs to be strategies at level of the government, industry sector and organization with focus on risk management and maintaining technology superiority for staying safe.

**SECURITY EVOLUTION AND TRENDS - BUSINESS PERSPECTIVE**

The management of security and its governance has become a highly complex task which requires a combination of technical, operational and business skills combined with meticulous planning and vision. The organization needs to address these challenges at three strategic layers of people, process and technology. Not only do organizations require competent people who can manage security, they also require an integration of skills beyond the traditional organizations boundary and structure. Here, it may be relevant to evaluate
capabilities possessed by firms specializing in cyber-security threat detection, analysis and mitigation. Such firms/individuals can help re-vitalize the enterprise risk management practice by helping the organization comprehend the daunting challenges associated with cyber security. Adoption of technology solves several business objectives; however, meticulous planning and oversight are required to help align business with security architecture. The solutions obtained by organizations need to be able to identify the context, content, complexity and relevance of information, thereby enabling granular control over information flow, within and outside the organization. Further, while processes help streamline operational activities across the length and breadth of the organization and their governance, they need to be agile to counter the ever-changing threat vectors and to tackle malevolent actors. The security function should also have representation in the boardroom and adequate resources should be made available. This will empower the security function to support business objectives and operational tasks with greater agility and confidence.

**SECURITY EVOLUTION AND TRENDS – TECHNOLOGY PERSPECTIVE**

The complexity in the IT ecosystems has increased manifold; however, businesses are in the process of recognizing the challenges and implement a holistic approach towards securing their operations. The security market is responding to these complexities with new technology solutions. However, deploying solutions alone will not ensure adequate protection and also get the RoI. Organizations need to develop and deploy well-structured and thought-out security architecture which leverages security solutions in a unified way to reduce risks. Organizations should develop a trust model, based on parameters such as content and context that allows only trusted systems to communicate. From an industry viewpoint, an example of trusted model could be creation of a private Internet ecosystem with strong inbuilt security and privacy controls. APTs are one of the biggest security threats today and to counter these, organizations need to build additional advanced capabilities including context aware data loss prevention capability, subscription to a security intelligence service, integration of security related events through SIEM type of solutions for delivering actionable intelligence, building network isolation, product trending and anomaly detection and sophisticated outbound firewall rules. Issue of security vulnerabilities in software products has been there for quite some time now, but still basic secure SDLC processes are not followed in many cases. New software product development methodologies such as ‘DevOps’ are emerging. These methodologies provide a good opportunity to integrate security across SDLC through automation and enhanced collaboration between different teams. Organizations should leverage such methodologies to enhance software product assurance.
Privacy landscape in India

Cross-border data flows – issues and ongoing engagements with EU & EFTA

Development of International Standards at ISO

Internet Governance & related issues

Development of Collaborative Protection Profiles under Common Criteria Recognition Arrangement (CCRA)

India’s participation in technical standard development- International Engineering Task Force (IETF)

With an aim to increase industry participation at national and international levels in domain of Security, Privacy, Internet Governance etc., DSCI organized a breakfast meet for AISS participants to apprise them about the engagements and opportunities, ongoing and futuristic, at all levels and how can they contribute in both individual and organizational capacity. Increasing industry participation will help voice industry concerns better and in turn improve overall cyber security and data protection ecosystem in the country and contribute in national effort of establishing India’s thought leadership in this ever evolving ecosystem. It also is in long term interest of security professionals and the industry to be more proactive in identification of issues and in influencing the developments of solutions through active participation and contribution. Above areas were covered as part of this exercise.
Cloud computing adoption has been growing steadily over the past few years and the momentum is expected to continue to accelerate globally across all sectors and enterprises. This paradigm shift in computing enables governments, consumers and business users to utilize ICT services at large scale with efficiency. However, the cloud is not entirely a new archetype - the ability to store, manage and retrieve data from hosted services having been in use for over a decade in various forms. What is different in the current paradigm is the sheer scale, and array, of services and applications that are powered by this new world of data and how they must now coexist in more complex political, regulatory, economic and social contexts. Interdependencies created by the distributed computing may hamper the capability of a nation in guaranteeing the rights of individuals, protect business interests and protect national interests. The situation is further complicated by the fact that most of the existing regulatory models were designed for a completely different computing environment. Without doubt, security and privacy are perhaps the most critical aspects of cloud policy development. Both of them are often seen as antithetical, akin to the two players of a zero-sum game. However, such a construct has also often been criticized as fallacious. One difference between the two is that security implies improper access to personal data whereas privacy more often implies its improper usage. It is challenging for the governments and policymakers in formulating cloud security policy - balancing the need to fulfill their national security/law enforcement responsibilities yet allowing the technology environment to thrive and deliver economic benefit.
KEY TAKEAWAYS

There is a growing trust deficit in the global community vis-à-vis usage of cloud services post Snowden revelations. The cloud ecosystem is highly dependent on trust and the revelations have undermined it. However, governments should avoid knee-jerk reactions and avoid taking regressive steps such as localization of ICT infrastructure. The underlying issues need to be addressed through a variety of measures. Governments need to be more transparent and open with respect to surveillance and interception and respect the privacy and human rights of the individuals. The international community could devise global norms for conducting surveillance.

There is a need to harmonize governments’ policies and regulations related to privacy protection, encryption standards, data breach notification, etc that impact cross border data flows and thus directly or indirectly regulate cloud services. In this regard, a model international law that governs cloud services can be created to harmonise different national requirements. Basis this law, countries can align their policies and regulations to promote cloud adoption. Also, countries should clarify existing laws and policies with respect to the Cloud.

There is no technology available that enables cloud service provider to classify data based on the certain parameters especially that could help classify data as lawful or unlawful and help cloud service provider comply with local laws based on data segregation.

Contract negotiation is a very important element of procuring cloud services. Many times, the SME organizations are unable to negotiate terms with large cloud service providers. To address contract related issues, a model cloud contract can be developed to achieve maturity in client–cloud service provider relationship. Such a model contract could include provisions related to liabilities in case of data breaches, right to audit, among others.

International, multi-lateral and bi-lateral agreements are required to promote free flow of the data across the borders and act as key enablers for cloud adoption. Such agreements should also create quick resolutions mechanisms (arbitration tribunals) to address any dispute or issues between buyers and suppliers of cloud services.

Cloud service providers should support law enforcement agencies of different countries in crime investigations (access to data records, evidence) and forensics. The support should be transparent and timely, respecting the laws of the country from where request has originated, irrespective of the location of the data storage.

Assurance schemes for third party certification of cloud services are not very mature and need to be promoted to enhance trust in cloud. Also, capacity building through training and certification of individuals is also an important aspect that needs to be undertaken on priority for creating a large pool of skilled resources.

Governments or organizations cannot address the security and privacy related issues in the cloud in silos. An institutional mechanism based on P-P-P should be created to build trust and maturity in cloud computing.
Globe-spanning reach of the Internet touches the lives of more than 1 billion people. Its benefits are extolled but is also prone to misuse – it has been used to establish superiority by nation states – for conducting espionage, surveillance, attacking critical infrastructures, etc. Its reach is expanding exponentially, and given its increasing role in our daily lives, concerns around issues in Internet Governance (IG) have caught eye of many. IG is one of the most hotly debated topics that are expected to dominate global discussions in time to come. The current arrangement and model of IG, and thus exercise of control over critical Internet resources, has been raising many questions. The emergence of institutions such as ICANN (and its prominent role in IG), and of intermediaries over the Internet has redefined governance – wherein non-state actors have larger say in how the affairs will be managed, making nation states helpless spectators. However, the relationship these institutions share with the US government (by virtue of their incorporation in the US and the fact that the Internet was born out of the US) has raised eyebrows, more so after Snowden revelations. Many countries see the collusion between US government and such institutions as unilateral control of the Internet by the US. Government and the world want equal rights in the governance of the Internet – and all related matters such as policy, technical, oversight etc. Countries such as China, Russia are known to exercising complete control over the Internet within their ‘territorial boundaries’ in name of ‘Sovereign Rights of Nations’. Brazil has too moved a resolution requiring setting up of Internet infrastructure within national borders. Global bodies, such as UN are also seeking proactive role in IG. Such multinational arrangements are seen as one of the alternatives to current arrangement that could help stabilize the IG mechanisms - else the fear of balkanization of the global Internet looms large.
The governments around the world are becoming uncomfortable with the way Internet is governed today – while the technical issues are non-controversial, policy issues are on the agenda of the governments, more so after Snowden revelations – they want to exercise their sovereign rights over the Internet resources.

In the present arrangement, though there are mechanisms in ICANN such as Governmental Advisory Committee (GAC) which provide opportunity for the nation states to highlight their concerns, their recommendations are not binding on ICANN and the ultimate decision making is with the ICANN Board which is not accountable to other nation states. Also, the US laws need to complied with - US government agencies or US courts have jurisdiction over ICANN operations since it is incorporated in US and not under any Host country laws that make it independent. The factor that a body which is managing affairs of Internet almost solely is governed by US law disturbs many nation states.

Though many of the global concerns are genuine, there are lot of legacy issues with respect to governance of the Internet. These issues exist by the virtue of Internet being invented in the US. Such issues are being addressed by the ICANN through different strategies & initiatives such as opening new offices in Singapore and Istanbul, setting up of ‘strategic panel’ to explore new governance models, considering re-allocations of root servers to some other global body where other nation states have equal say, and registering itself as a non-governmental body in Geneva, among others things.

Post Snowden revelations, nations have come together to condemn sweeping mass surveillance – the recently passed UN resolution ‘privacy in the digital age’ is a testimony of that. While there is a need to create new global treaties and conventions, the existing ones must be reviewed to assess their effectiveness and utilization – Mutual Legal Assistance Treaties (MLATs) is a case in point. When such treaties don’t work, the nation states may resort to other solutions which can harm economy, industry, society and consumers in the medium to long term.

To resolve the governance issues, some countries have suggested that the ICANN operations be taken over by UN or ITU. This suggestion does not seem to be acceptable to many stakeholders, including the US and ICANN, as they fear that elevated intervention of governments will kill the laissez faire spirit of the Internet and the private sector, technical communities, academia and civil society (who all have played pivotal role in making Internet what it is today) will not be on equal footing with the governments in UN setup.

The control of the Internet has been unilateral so far but post Snowden revelations has sparked a global debate on who should govern the Internet and how should it be governed. There are two schools of thought – one favouring multi-lateral governance of the Internet, which gives more say to the nation states; other focuses on multi-stakeholderism which advocates participatory governance of the Internet involving all stakeholders including governments, industry, academia and civil society. The critics of the former school of thought state that it is not possible for governments to agree on contentious issues, while the critics of latter question the feasibility of involving so many stakeholders to make decisions.
While the ICANN tries to establish itself as a neutral independent international non-governmental body, global norms need to be codified for Internet governance which provide directions and guidance for nation states to act, else the sovereignty issues will remain unaddressed. Any such global norm must recognize the role of different stakeholders including the private sector, technical communities, academia and civil society by making multi-stakeholderism the underlying principle. In doing so, defining ‘multi-stakeholderism’ and how it works is extremely important. The body responsible to manage Internet resources, whether ICANN or any new entity created, should be subject to International law and overseen by an international appellate (e.g. for dispute resolution), comprising of experts sponsored by respective governments.

The global solutions that may emerge should strive to create necessary balance in cyberspace between freedom of expression and restrictions, national security and privacy, among others with the ultimate objective of welfare of the mankind. Such solutions should create a level playing field for all stakeholders. To enhance trust in cyberspace, governments should enhance transparency and be more forthcoming in sharing information with relevant stakeholders. On the other hand, in establishing sovereignty, nations must not create hurdles for economy by demanding localization of ICT infrastructure, restricting trans-border data flows, among others.

India should deliberate the issue of governing cyberspace more comprehensively and increase participation and representation in global bodies, committees and forums to voice local concerns in a better fashion. The brainstorming should start within the government with inter-ministerial consultations and consultations with industry, civil society and academia should take place on a continuous basis. This will help in formulating India’s position in international discussions and negotiations regarding governance of cyberspace. Internally, more conferences, workshops and seminars on this issue should be held to raise awareness and outreach among the masses.
Critical Information Infrastructure (CII) includes physical assets connected to cyber, cyber assets, networks and systems that are integral to the functioning of a nation. Its protection is warranted to maintain national security. CII owners, largely in private sector, are still struggling to protect, withstand and swiftly recover from cyber attacks due to variety of reasons – no clear mandate & policy guidelines from governments on CII protection, organizations inability to replace legacy systems, hardening and patching not implemented religiously in organizations, exploitation of human gullibility, lack of sensitivity towards critical systems, dearth of sector specific standards and regulations, inadequate integration of CII in nations cyber preparedness system which includes prevention, protection, mitigation, response, and recovery. We are a part of cyber kinetic era now which in the past was considered purely fictional. There is a growing realization that the kinetic impact of cyber attacks can result in physical damage, casualties or even death via exploitation of critical infrastructure, systems and operational processes.
The incident of stuxnet in Iran validates the concept of kinetic impact of cyber attack as it damaged the centrifuges at one of the fuel enrichment facility. It damaged cyber physical systems (CPS) of the nuclear facility resulting in its malfunctioning.

Global security community needs to realize the cyber threat posed to critical infrastructure connected to cyber or which runs on intranet or internet and also associated with other systems. If ignored, it may lead to large scale and non-recoverable impact of cyber attacks on CII, resulting in loss of confidence and trust on technologies. These apprehensions warrant building a separate threat matrix for CII.

Cyber physical systems are designed in such a way that they can establish control and can be monitored via IT systems and this functionality makes them vulnerable to kinetic impact if not protected efficiently. CII organizations need to compare each other’s security best practices with respect to ‘controlling & monitoring of CPS’ to build a robust secure environment.

CII organizations need to conduct critical examination of how the operational technologies work, how these technologies are evolving and marrying with the Internet technologies, and how they have been deployed for strengthening the CII cyber ecosystem. Also, special focus should be there to address the ICT supply chain risks in such technologies.

The owners of the critical infrastructure can position CII cyber security in a way that they are able to manage risks in their respective operations and further collaborate with other owners to address risks that may exist due to interdependencies between critical infrastructures.

The security community needs to find answers in terms of technology capabilities, robust cyber policies, standards and regulations. As the cyber attacks on CII may create long lasting kinetic impact on nation’s infrastructure and may lead to conflicts within nations, they deserve attention from the perspective of international conflict resolutions. The global community should work towards developing international agreements, norms or resolutions to avoid such cyber conflicts.
The global economy and a nation’s critical infrastructure rely on the Internet for communication and connectivity. Telecommunication networks act as the heart of interconnect between various industries, organizations, countries etc. However, the Internet traffic, in addition to genuine datapackets also contains spurious/malicious traffic like spyware, malware, worms, trojans, etc. This not only compromises security of data but also chokes up the bandwidth. With their unique vantage point over the organizations’ networks, telecom firms are ideally placed to deliver “clean pipe” Internet service by curtailing external network threats before they reach their customers’ endpoints. However, in doing so there are several challenges including policy, legal, administrative, cost, technology, privacy and user awareness.

Global ICT supply chain security remains an area of concern for telecommunication in India, as operators and service providers rely on globally sourced equipment and systems. These systems may inherently have vulnerabilities which may be exploited to propagate malicious traffic through the telecom pipe. It is thus essential that all equipment and systems which constitute a telecom network and help establish the telecom pipe are designed and tested based on globally accepted standards.

Many end systems are compromised by trojans such as bots. These are exploited by bot owner who uses them to cause DDoS attacks. The level of sophistication and functionality of botnets has experienced a drastic advancement in the recent past. It started relying on P2P technologies and the establishment of a distribution network which is laid across several countries. Botnets for mobile networks have also started to emerge. A mobile version of the Zeus trojan targeted multiple mobile platforms and was successful in by-passing SMS two-factor authentication, resulting in theft of banking data using mobile transaction authentication numbers.
A methodology which may help mitigate DDoS attacks involves the use of traffic collectors which aggregate samples from routers. This traffic is sent to a scrubber which analyses the traffic and extracts the obnoxious traffic. While this helps in evaluation of DDoS attacks, the complexity of this process varies on the type of networking device installed by the telecom service provider and results may vary on the capability of the equipment. However, the customer has to consent to such traffic analysis.

Countries that do not have adequate national policies and legal framework for cyber security and crimes become safe havens for the bot networks. Nations should empower the respective machineries with necessary powers to take actions. Nations should have active operations in identifying and taking down the bot networks. For this, governments and industry should collaborate at national and international levels. Necessary international collaboration should be established via CERTs or other agencies and programs.

The Department of Telecom (DoT) through the UASL amendment has mandated audit of all telecom equipment by a third party auditor in addition to seeking a self-certification from the telecom operator. The system upgrades and patches also need to be designed and configured using safe security practices. Appropriate security evaluation of all equipment must be performed by testing and simulation prior to their deployment in a live environment. The operator must conduct timely intrusion detection tests and report to the CERT-In, in case of detection of malware or malicious traffic.

Existing regulations expect snapshots of the system via timely audits and checks; however, what is required is a continuous evaluation of threat vectors. Unified threat management deployed in the cloud may offer protection against such threats as the traffic may first be scanned in the cloud prior to being delivered to an organization. The cost of such offerings may be prohibitive for individual customers however it may be relevant for businesses to opt for such services. Managed security service providers ecosystem in India needs to evolve further.

List of infected devices runs into thousands and it is easier to protect devices from infection at the operator level rather than contacting each customer to individually clean systems. However, the most effective approach will be to educate end users about the need to clean their systems. Education and awareness to end users is of utmost importance as they form the source of compromised systems. Combined with telecom operators contributing to control of malicious traffic, we may hope to achieve reduction in spam and botnet infected systems.

Traffic may be intercepted at the gateway level and landing stations in India and a rule based system may be configured to terminate traffic at the gateway level. However, this traffic is in terabytes and currently there is a lack of devices which may analyze this huge amount of traffic against its rule base on a real time basis. Hence the role of telecom service providers becomes increasingly important as they distribute this traffic across the nation. Deep packet inspection technology may help by inspecting traffic down to the application layer. However this may create huge concerns in terms of privacy and will also lead to introduction of delays in traffic delivery.
Story so far...

Global market has witnessed confidence on the Indian security companies. Increased export revenue.

Core R&D work, diverse product portfolio, enterprise level products & global recognitions.

Emerging and sustaining itself in the market of established payers.

Success stories, global acceptance, retention of clients, gives testimony of competencies.
ADVISE TO ASPIRANTS

Key to achieve success on path of entrepreneurship: Strong passion and faith in the idea and courage to take it forward.

Hear yourself: Don’t go for something where others are doing well. Success resides in one’s own domain of expertise.

Innovation culture: Promote the culture of innovation, give freedom, empower team and have a room for mistakes.

INNOVATION & ENTREPRENEURSHIP ECOSYSTEM

Entrepreneurial culture is need of hours in the domain of cyber security.

Special drive to cater need of security research, development & entrepreneurship in the country.

Enhance adaptability to new experimentation, innovation & solutions by buyer community.

Access to funds and capital, enabling market drivers & healthy investment culture.

GOVERNMENT’S ROLE

Platforms for capabilities demonstration in government to build trust in becoming part of public procurement.

Government as a buyer of the indigenous offerings. Public procurement rule and procedures should enable it.

Expansion needs global exposure- government to help in reaching out to new markets.

Skills and capability building in R&D, product architecture and engineering.
100+
THOUGHT LEADERS
100+
THOUGHT LEADERS
SECURITY & PRIVACY AS A CAREER

1. GLOBAL PERSPECTIVE
Skill requirement number in security is always difficult to come by.
Characteristically there is always underestimation of numbers, shortage in the skills is huge.
Need of forensic skills is growing by 30 to 40% across the globe.
Industries such as Health care, Telecom awakening to security challenges.
1 million certified people needed in health care industry alone.

2. NATIONAL PERSPECTIVE
Security is complex subject, there isn’t much comprehension available.
Malware reverse engineering, application security, countering denial of service attacks, log analysis, botnet detection & visualization, mobile security, forensics... are the key capability areas.
Skill building in security is adhoc in nature.
Singapore talks of 1% security professionals, US rise in security professionals growing by 28%.
India needs 500,000 security professionals.
Skill building needs cutting edge technology, composite career plan, compatible culture and continuous education.

GLOBAL NATIONAL
SERVICE PRODUCT
3. SERVICE INDUSTRY

Many universities in India offer M.Tech/ MS course in security, there are about 80 of them in country

Dimensions of requirement- Security, risk, law enforcement, compliance and operations

Conceptual understanding is the key in entering in the field

Starting from simple scan, one can grow in various level

Thousands of people needed in security, globe is looking to India for supplying the skills

Indian companies involved in capacity building exercises in various other countries

Technical security architects are in dire need, but very difficult to get

4. PRODUCT INDUSTRY

Core engineering talent - programming in C/ C++ and operating systems

Core engineering like operating system not taken seriously, security research ties to the core skills

Product company has to invest training as existing ecosystem is not able to create these skills

Sales engineering and support requires different skills

Threat research is an interesting area, conventional education may not be generating that

In the age of cyber war, the country needs key skills to tackle the challenges

KEY TAKEAWAY

Country needs key capabilities in encryption or developing operating systems

Local level efforts for changing syllabus may not yield desired effect, syllabus change for developing critical skills need national level push

Career path of security at higher level is bit difficult, can CISO aspire to become CEO

Open source online education will give the access to critical global education

Capacity building in security requires national level framework
The “free” Internet but has a price. Every second there is a huge amount of data that users upload about their activities; they conduct transactions over the Internet, email contacts or read about political developments in their country. However, this seemingly private data of our activity is captured every bit and is available to be analyzed by governments and organizations, who obtain that capability. Governments across the globe have realized the benefits of mining data for the purpose of national security. However, surveillance creates an imbalance if this data is used for discrimination or it is misused for personal reasons, thus harming residents of a nation.

While most legislations and regulations, at the moment, protect people’s privacy from companies and governments, the need of the hour is to prepare for an age in which, simply by living their lives, people create vast searchable records and individual databases through the use of upcoming technology; an age where advanced sensors are imbibed in the daily fabric of human existence, an age where advanced algorithms start predicting our every thought and action. In this age of large scale analytics, enabled by big data, the biggest causality is privacy. Big data changes the entire paradigm of privacy to a very different level, even raising doubts about the futility of such a discussion in this age.
Technological advancements have revolutionized the way we operate, the way we live and now also impacting the way we behave. From huge, bulky supercomputers which would occupy the entire room and performed very limited functions to the age of social media, cloud computing, analytics and mobility gaining traction to proliferation in use of sensors and chips that are used to read, track individuals where every device would get online to Internet of things that speak to each other to use of technology that helps capture thoughts and even modify how you think, technology has certainly come a long way and now very much an integral part of our lives in everything we do. The benefits of technology are extolled. Counter view is that we have become technology slaves and may no longer lead life of our own as technology becomes too intrusive, governing how we react, behave and think.

Technology can act as both boon and bane – depends on how we use it. Privacy as a concept gained traction due to massive data collection by the states but now even private sector has the capability, and might have even surpassed the capacity of data collection. All kinds of business models, harnessing personal information for delivery of goods and services are shaping up on daily basis. Economic value of data has risen but due to lack of awareness amongst citizens with respect to their rights, people often trade their personal information, usually voluntarily, in lieu of benefits.

Information is generated, disseminated and collected in real time. The ability to generate such data, as never seen before, would also impact on how we use such information and how it in turn impacts privacy. Sensors are used to track habits and behaviors and such information can be used for variety of purposes – in manner that both make our lives convenient and also that impacts privacy. In current technology age, and also in time to come, how will such changes impact privacy principles, how will these be of relevance to privacy and how privacy will be enforced amidst everything is to be seen.

Use of technology, even in an intrusive manner, used for public good, for providing services in regulated manner, with consent is one thing against it being used surreptitiously, without consent, for personal benefit is another thing. Wearable devices and gears, example glasses with sensors, can help gain knowledge and insight with real time information and develop deep understanding of things that one sees. But at same time, it can be exploited to look up people, record their daily motions, track and profile them, and gain information about them thereby intruding their privacy. Do privacy principles such as notice, choice, consent etc. have relevance in such scenarios?

Vint Cerf says ’Privacy may be an anomaly in present age’. Lack of awareness amongst users also is an important factor leading to privacy being impacted. However, importance of privacy cannot be ignored as it gives freedom of individual expression and lead a life of personal choices which is away from scrutiny and lead to growth. Studies have established that individuals do not behave normally, when being monitored or tracked. Hence, for growth of individuals and society, privacy has to be established. A balance needs to be struck on what is acceptable and what is not.

**KEY TAKEAWAYS**

- Technological advancements have revolutionized the way we operate, the way we live and now also impacting the way we behave. From huge, bulky supercomputers which would occupy the entire room and performed very limited functions to the age of social media, cloud computing, analytics and mobility gaining traction to proliferation in use of sensors and chips that are used to read, track individuals where every device would get online to Internet of things that speak to each other to use of technology that helps capture thoughts and even modify how you think, technology has certainly come a long way and now very much an integral part of our lives in everything we do. The benefits of technology are extolled. Counter view is that we have become technology slaves and may no longer lead life of our own as technology becomes too intrusive, governing how we react, behave and think.

- Technology can act as both boon and bane – depends on how we use it. Privacy as a concept gained traction due to massive data collection by the states but now even private sector has the capability, and might have even surpassed the capacity of data collection. All kinds of business models, harnessing personal information for delivery of goods and services are shaping up on daily basis. Economic value of data has risen but due to lack of awareness amongst citizens with respect to their rights, people often trade their personal information, usually voluntarily, in lieu of benefits.

- Information is generated, disseminated and collected in real time. The ability to generate such data, as never seen before, would also impact on how we use such information and how it in turn impacts privacy. Sensors are used to track habits and behaviors and such information can be used for variety of purposes – in manner that both make our lives convenient and also that impacts privacy. In current technology age, and also in time to come, how will such changes impact privacy principles, how will these be of relevance to privacy and how privacy will be enforced amidst everything is to be seen.

- Use of technology, even in an intrusive manner, used for public good, for providing services in regulated manner, with consent is one thing against it being used surreptitiously, without consent, for personal benefit is another thing. Wearable devices and gears, example glasses with sensors, can help gain knowledge and insight with real time information and develop deep understanding of things that one sees. But at same time, it can be exploited to look up people, record their daily motions, track and profile them, and gain information about them thereby intruding their privacy. Do privacy principles such as notice, choice, consent etc. have relevance in such scenarios?

- Vint Cerf says ’Privacy may be an anomaly in present age’. Lack of awareness amongst users also is an important factor leading to privacy being impacted. However, importance of privacy cannot be ignored as it gives freedom of individual expression and lead a life of personal choices which is away from scrutiny and lead to growth. Studies have established that individuals do not behave normally, when being monitored or tracked. Hence, for growth of individuals and society, privacy has to be established. A balance needs to be struck on what is acceptable and what is not.
The increased adoption of social media, mobile phones & cloud, the inherent vulnerabilities and criminals targeting exploiting such technologies and vulnerabilities, stipulate an understanding of how digital forensic investigations can be performed. For instance, today banking institutions have started encouraging users to perform online financial transactions on social media sites. This kind of activity involves many intermediaries which may be located globally, making digital forensic investigation an arduous task.

Today, there exist thousands of smart phone applications which may hold critical information required for conducting investigations. The forensic tools support for the smart phone applications have begun in the last few years only and cover only popular applications. Privacy issues have always remained a major concern in digital forensics. Unlike the physical world, the digital space generates a huge amount of private data that makes it impossible to offer full protection during the transfer, storage and collection of data. The forensic investigators are facing challenges in finding the balance between retrieving key evidences and infringing user privacy.
KEY TAKEAWAYS

- The companies are facing issues with their employees misusing the social media sites; this should not be dealt with technical controls and restrictions. Social media usage policies need to be created and awareness among the employees needs to be created.

- There are no established procedures in dealing with the cloud forensics today. Data is being backed up in multiple locations, in many cases, without the client’s or user’s knowledge. One way of overcoming this would be to have a Service Level Agreement (SLA) with the service providers to provide access to the snapshots (freezing the data at a particular point of time) in case of a criminal investigation. This legal backing would help the law enforcement agencies in dealing with offenses committed using the cloud environment.

- The cloud environment doesn’t, in many cases, provide physical access to the digital devices to examine artifacts related to an investigation. Under such circumstances, the data that is essential for a digital investigation should be collected proactively by the cloud service provider to help the investigation agencies.

- Maintaining the chain of custody of the digital evidence on a cloud, social & mobile environment is as important as in any other environment. The judiciary should be made aware about the importance of digital evidence handling to encourage the admissibility of digital evidence.

- There is no harmonization of policies with respect to sharing of information by service providers, especially that are based out of India. Multiple jurisdictions mean multiple legal regimes and there are some efforts taken by the relevant international agencies for providing the trans-border access to stored computer data. One such effort is the Budapest Convention-India is not yet the signatory to this convention.
PROBLEM DEFINITION

Nation states have increasingly started giving due emphasis to ‘Cyberspace’ and treat it at par with other domains – land, air, sea and outer space. There are about 35 suffixes that are used with the word ‘cyber’, and importantly cover words such as warfare, strike, attack, espionage, terrorism etc. that have become one set of most used words in recent times. What began as fiction in Hollywood movies is slowly and steadily acquiring a real face. Attacks have constantly been on rise, with proportion of state sponsored attacks increasing rapidly. Nation states have been developing cyber offensive capabilities.

More than 150 countries are in the process of developing cyber offense capabilities, as reported by a security research company. Cyber attacks provide an unprecedented opportunity of causing big impact to adversaries with minimal efforts. The unique feature and character of the cyberspace is increasingly attracting attention of state and non-state actors. Anonymity, the very basic characteristic of the Internet that fuelled the innovation, has made cyberspace as an easily exploitable conduit in a deceptive and covert way. The recent revelation of major attacks such as Stuxnet, Flame and Nitro attack confirm the fear about the ability of cyber space in compromising security of a nation.

Whether cyber warfare is a reality or hype is still debatable, but it is universally recognized that the cyber capabilities will play essential role in supporting other forms of warfare. Every sound defence needs to have offensive components and that is the pretext used by nations to develop offensive capabilities.
No global arrangement that recognizes and defines rules of engagement for cyber warfare exists. The closest doctrine that can be considered is the nuclear doctrine. Additional Protocols of Geneva Convention and Law of Armed conflict exist, but are not specific to cyberspace. Nation states and global bodies are still in discussion phase and exploring ideas to come to a conclusion. They don’t want to engage in premature consensus as the same nations are looking it as a medium to exploit, in absence of global norms and treaties. There is even no universally accepted definition of cyber warfare and therefore countries have their own understanding of the term cyber warfare. IDSA Task Force defines it as an action by a nation state or its proxies to penetrate another nation’s computer or network for purpose of espionage or disruption.

Cyber attacks and espionage used as component of cyber warfare are regarded as ethically and morally wrong but still in use by nation states, as part of statecraft to gain strategic advantage over enemies – analogous to use of spies.

The conventional warfare has been associated with violence, capability to force enemy to comply and inclination to achieve a political goal. Till date, no cyber attack has fulfilled all these dimensions. However, if one considers a different understanding of the term warfare which is more contemporary and evolved - where the act of war is not too focused on physical violence but also includes ability to cause economic loss, spread social chaos and dominate culture, then perhaps cyber warfare can be considered as a form of non-conventional warfare and a sub-set of information warfare.

Technology development influences conventional warfare. For instance, the invention of airplanes, saw induction of fighter planes. Cyber warfare is regarded as fourth generation of warfare that is asymmetric, often regarded as ‘No contact warfare’. And it is also different as the resources that are used to fight cyber war extend beyond the two nations that have indulged in cyber war – third country might not even be aware that its resources are being exploited to launch attack on another country.

Similarly, development of cyber technologies will influence warfare and nation states will pursue such technologies to establish superiority. In the past, nuclear weapons have been used by nation states to establish their superiority and the acquisition of this capability has deterred nations to engage in conventional warfare. Given the reduction in conventional wars, cyber weapons can be strategically and stealthily used for conducting espionage, attacking critical information infrastructure, creating social chaos, etc – similar to how terrorism has been used by nation states to launch a proxy war.

The main objectives of pre-emptive cyber strike are ‘Strike your enemy before he is ready’ and ‘Deterrence by denial’ – deny your enemy to attain certain capabilities and stop him in his track. The first strike is crafted to deliver a deafening blow and take down countermeasure or retaliatory force and even disrupt cyber offence to negate chances of strike back. Lethality & obfuscation are kept in mind while delivering strikes.
Whether pre-emptive strikes are justified or not depends on lot of parameters – context of strike, circumstances, objective & aim, target etc. For an example, if it is a matter of survival for a state or its infrastructure is presumable under serious threat from another nation, will it be justified? A thin line exists that delineates justification. Pre-emptive strikes often lead to conflict escalation model and goes into spiral with constant retaliation through different modes or channels. It is analogous to a chess game where you make your move and wait for opponents move before you make another move.

Whether a cyber-attack can have a kinetic impact or not – only time will tell. But the risk is not overstated - one must not underrate the potential of cyber capabilities. It may be argued that cyber warfare cannot be considered as a separate domain of warfare but as with other inventions and technology advancements, superiority in cyber technologies should be achieved to stay relevant in the world order.

Cyber warfare is not only restricted to military operations or actions of federal governments. P-P-P in this realm is also being witnessed. There needs to be a strategy at level of government, industry sector and organization with focus on risk management and maintaining technology superiority against your counterparts to stay ahead in the game. India is under continuous cyber threat and is vulnerable too. Therefore, India must focus on building defensive and offensive cyber capabilities. A body at joint services level and at each service level exists to protect against external threats and prepare for attacks, but with limited resources and operations. India should also develop a cyber warfare doctrine in which it should define the threshold till which the impact of cyber attack can be tolerated without retaliation.

A global agreement or arrangement should be made to classify defensive and offensive cyber technologies and control the development and usage of cyber offensive technologies by nation states.
A security breach may not only cause loss of information and data, but also have a daunting financial effect, loss of reputation and confidence, which may lead to an overall decrease in trust, litigation or lead to adverse conditions for the organization. Traditionally, information security has focused resources to keep all assets within the environment of the organization by building secure firewalls to ward off any attacks. However, with an evolving threat landscape there may be several vulnerable attack points, which make it imperative for the security function to be revitalized. Advance persistent threats are a reality and newer means to exploit vulnerabilities in systems and networks are being discovered each second. Organizations need to discover means to gain intelligence from internal as well as external sources and need to aggregate information and correlate it to derive valuable intelligence in near real-time for solving daunting security issues. To stay ahead of the evolving security threat curve, organizations need to be proactive, rather than being reactive to incidents and breaches.
The goals of the information security program need to be aligned with business goals and targets, which further need to reflect in the governance, risk and compliance frameworks adopted by the organization. The security function in effect should be able to provide measurable, efficient and consistent information to business stakeholders. On similar lines, risk assessment methodology needs to be reviewed to include parameters for information security and its governance. The real benefits of a robust security framework and practices and the return on investment made on security may not be directly realized; however, organizations need to understand the importance and value of robust security architecture by evaluating the additional, avoidable costs which the organization incurs after an incident occurs.

KEY TAKEAWAYS

The innovative use of technology to aid businesses has led to the introduction of inventive models of selling and serving customers. This leads to an expansion of the organizations footprint across a diverse geography and creates multiple touch-points for the consumer. However, each touch point remains a concern, as they offer potential for malicious agents to break-into the enterprise network.

The management of security and its governance has become a highly complex task which requires a combination of technical, operational and business skills combined with meticulous planning and strategic vision. It is thus essential that security practitioners align their practices with business goals and aspirations. Similarly, it has become imperative for business decision makers to accept security as a business enabler and help with effective security governance, risk mitigation and allocation of adequate resources to achieve security tasks.

The risk assessment of a typical organization revolves around identification of risk from operational and business related activities. However, with the increasing adoption of technology to achieve complex business goals and the expanding nature of the organization; the magnitude of threats and associated vulnerabilities has also intensified. Organizations are embracing technology such as cloud computing, adopting social and mobile channels to aid a mobile workforce. Thus the attack surface has grown beyond the reach of conventional security technology and methodologies.

Advances Persistent Threats (APTs) are designed to impact organizations in a highly covert manner, leading to theft of organization’s data and causing disruption over a long period of time. They may also mutate and adapt themselves in-order to evade detection. Such attacks are typically targeted at organizations holding sensitive information with impact on national security or information which is confidential such as Intellectual property and trade secrets. However, defence and protection against such threats requires greater co-ordination between business functions along with a proactive security methodology which combines both internal and external intelligence.
Protection from advanced threats also calls for building greater visibility over the type of information that flows over the organization's network, the context in which the information is accessed, the people who handle information over its lifecycle, the devices which connect to the organization's network and the applications and processes which are operationalised within the organization amongst others. Such visibility would be essential for developing a defence mechanism and in conducting risk assessment for the purpose of information security.

Deployment of security capabilities which are agile and responsive to the changes in the business objectives or requirements are necessarily a first step towards protection from advanced threats. Organizations also need to focus on building and enhancing the competence of personnel deployed in the security function, along with communicating the importance of following safe practices to all employees and third parties. There also needs to be specific focus on governance of all activities as part of the security function, to ensure co-ordinated planning, assessment, response and compliance.

The objectives of Governance, Risk Management and Compliance (GRC) are more inter-aligned than ever. Typically, all three have been executed with the intent of helping businesses achieve lower cost, increase synergy and provide transparency to stakeholders for effective business decision making. The GRC functions now have a new perspective, with the aid of technology. Data about every activity, touch-point, process and procedure is made available for stakeholder's consideration and action, providing them a single view to keep track of and check health status of the operations.

While such vast amount of data empowers decision makers, IT systems need to be designed with the objective and capability to respond to granular policy based changes, while ensuring adequate automation such that interdependent actions are auto-adjusted in near real time. This is also true for security systems and appliances, which need to be adaptable in-line with changes in business decisions. The three stages of GRC solution information management namely, information infrastructure, information intelligence and information governance, can help in achieving standardization, reduce duplication of efforts and develop common vocabulary for asset infrastructure, develop better transparency and visibility across all layers of operation, and formulate unified approach to help take steps proactively and manage issues more effectively.

In addition to revitalizing internal structures and processes, organizations also need to enhance their capability to counter risks and vulnerabilities by integrating services of external service providers, who specialize in tackling such risks. Criminals and malicious agents, after the organization's information, are highly skilled and collaborate openly across the globe. The threats which organizations face are no longer local or restricted to the geography of its operations. Threat actors seek support and collaborate extensively, thereby executing attacks which are not only difficult to evade but also challenging to investigate. Thus organizations need to augment their security frameworks and capabilities with the addition of external individuals and firms, which provide proactive defence.
Information security is a trade-off - a balancing act between perceived risks and organizational resources. Maintaining this balance is challenging as the threat environment is very dynamic. Evolution of technology impacts both sides risks and resources. Organization has tries to induct new technologies to address the risks and on the other hand cyber criminals or rogue insiders utilize the same technology to conduct attacks. Organization has to defend against every possible attack, while the cyber criminals or rogue insiders have to find only one loophole to penetrate the defense. IT ecosystems in organizations are getting more complicated due to technology evolution such as proliferation of smartphones and associated applications, integration of cloud and non-cloud based platforms, role of big data analytics, enhanced network ability to handle millions of devices, among others. This implies birth of digital revolution which enables businesses like never before, but which also introduces complex security issues. Fortunately the security market has responded to address such issues. The security technologies have evolved with the surfacing of trends such as architectural solutions to block APTs, implementation of trusted networks and trusted computing which may lead to obsolescence of traditional security capabilities, transformation of IT operations and governance with the help of DevOps, Optimizations of SIEM capabilities for next generation defense, among others. These latest trends are yet to be understood completely by the organizations and till the time that happens, cyber attacks are expected to continue. The outcomes of these evolutions are trying to find their place in the larger defense structure. Security technology trends which are emerging warrant organizations to build capabilities to understand how the security ecosystem is changing and deploy security technology solutions in a structured manner to safeguard against possible risks.
The complexity in the IT ecosystems has increased manifold; however, businesses are in the process of recognizing the challenges and implement a holistic approach towards securing their operations. Currently, there is an adhoc adoption of security solutions to plug gaps in the security cover. This has led to a non-standardized security architecture which is inadequate to deal with the security challenges and the evolving threat landscape.

Businesses are driven primarily by regulatory bodies, government agencies and client requirements. Such drivers help address security challenges in the short term, but fail in ensuring that security imperatives are taken up by businesses in a proactive manner.

A typical antivirus approach will not protect against day zero attacks. Based on historical analysis we may blacklist traffic and stop threats. However, this needs to be updated more rapidly now than ever. The emergence of the whitelist approach – to only allow trusted systems to communicate – and establish a default block all may help establish trust between devices and interconnected systems.

Trusted computing ensures only authorized users and authorized PCs are on an enterprise network. It also acts as a secure vault for certificates, keys and passwords, negating the need for tokens. It also interfaces various technical standards to create an end-to-end enterprise solution that is tailored to meet mission and business needs and comply with security policies within public and private cloud networks. Trusted Network Connect (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC provides pervasive security, Network Access Control (NAC) and interoperability in multi-vendor environments.

There are two essential approaches in building trust – first, to consider the IT ecosystem which involves multiple devices and vendor environment and second, the network ecosystem which acts as interconnect between all devices, systems and vendors. This calls for identification of parameters which may be used to build a trust model for devices and systems to communicate. The key parameters of trust revolve around context and content.

To address the trust issues, especially in the case of critical transactions over the public network, control over the security of the transactions has been acquiring the attention of businesses. Industry verticals such as financial sector can create a private internet ecosystem with strong security and privacy considerations from technology as well as process point of view, to gain the traction of the users and establish trust.

From the user industry perspective - integrated, standardized security appliances and applications along with a unified SOC which address challenges of scalability brought about by technology such as virtualization need to be developed.
In public networks that provide a platform for interaction and exchange of information to the end users, trust is the key driver and enabler too for its adoption to carry out critical transactions. Recent revelation of NSA surveillance and access to the private data of global citizens on the Internet has emerged as a serious global issue, and has adversely impacted the level of trust on the public Internet. In the wake of such revelation, organizations need to gain trust of users to sustain their businesses. There should be some mechanism of certification or third party audits so that confidence of the users can be enhanced.

The combat against APTs can start from assessment of present defense systems to identify gaps and left out systems, upgrading critical security processes and technologies and last but not the least giving equal attention to forward leaning capabilities and processes when trying to mitigate APTs. To counter APTs deployment of additional advanced capabilities may include data loss prevention capability, subscription to a security intelligence service, integration of security events, network traffic and communication flow capabilities, building network isolation, product trending and anomaly detection and sophisticated outbound firewall rules.

SIEM solutions typically try to correlate the instances to identify the patterns in real or near real time. They have to deal with huge set of contextual data, which may generate noise if not properly handled. The slow and covert operations of the threat agents in many instances escape detection. Low profile operations may not generate enough signals which can be detected and correlated with other instances.

SIEM solutions need contextual intelligence to address all possible dimensions of complexities. It has to deal with a complex set of historical data, and correlate with the current context. It has to deal with various sources of information, structured and unstructured and that too in large sets. SIEM solutions need to be effective by learning to deal with plethora of information. They have to be transformed to deliver intelligence driven security.

Philosophy of the DevOps started with the concept of agile development, warranting strong collaboration between development and operations teams. This collaboration helps in achieving the required level of security and privacy in the system developed under the DevOps.

To address the changing business requirements, DevOps utilize emerging technologies to automate various processes across the life cycle of the development and deployment of software. For effective and efficient delivery, it is essential to have a composition of the team with required skill set, which also includes security experts.

It is said that “complexity is the enemy of the security”. In case of DevOps, complexity of configuration management, monitoring of security level in the product development and deployment can be arduous challenges to address. These can be addressed by incorporating requirements at the initial phases of design so that are addressed in a structured and timely manner. DevOps team should also be aware of the user interface (UI) features for any given types of users, infrastructure changes and other changes in the compliance requirements. This is extremely important to establish a seamless flow of information among all the stakeholders.
UNDERLYING TECHNOLOGY TRANSFORMATIONS

- Machine understanding human software defined environment-platform independent programming
- Accessibility of IPR information
- Device proliferations- smaller, smarter & embedded
- Institutional management of information
- Sensors, augmentations & algorithms
- Productive & proactive analytics & intelligence
- Internet of things, creation of multiple layers of information
- Measured & reliable remote processing
- Availability of context & context processing capability

TRENDS 2020, SHAPING SECURITY

- 3D Printing
- Body insertion of intelligent & connected medical
- Driverless cars
- Augmentation technology
- Thought driven actions
- Location intelligence
- Internet of Things
**KEY RISKS**

- Multi core chips, one core is malicious
- Embedded applications planting security vulnerability
- Internet of Things will make problem of vulnerabilities saviour
- Tampering at hardware & chip level to facilitate stealing & spoofing information
- Privacy issues stemming out of information management

**SECURITY EVOLUTION**

- Human components in security will go down
- Security operations are increasingly automated
- Security will be critically dependent on ability of process contextual information
- SDE may make OS, middleware, etc. irrelevant

**MANUFACTURING/PRODUCT | 2020 USE CASE**

**(3D PRINTING)**

- Printable design information is like source code
- Remote printability enhances IPR value significantly
- Potential to loose IPR will be more
- Business from components will diminish
Unfolding story of the Change Agents since 2011

WINNERS OF DSCI EXCELLENCE AWARDS 2013

Corporate Segment

DSCI Excellence Award for Security

Bank: HDFC Bank Ltd.
Telecom: Reliance Communications
e-Governance: UIDAI
e-Commerce: Ibibo Web Pvt. Ltd. (B2C)
National Payments Corporation of India (B2B)
IT Services-Large: Polaris Financial Technology Ltd.
IT Services-SME: Broadridge Financial Solutions (India) Private Ltd.
BPM–Large: Genpact Ltd.
BPM–SME: Quatrrro Global Services Pvt. Ltd.
DSCI Excellence Award for Privacy
Bharti Airtel Ltd.

DSCI Excellence Award to Information Security Product Company
Cyberoam Technologies Pvt Ltd.

DSCI Excellence Award: Security Leader of the Year, supported by RSA
Arun Kumar Anand, NIIT Technologies Ltd (IT sector)
Raja Vijay Kumar Adapa, Genpact Ltd. (BPM Sector)
Shanmugasundaram Ramasamy, Indian Oil Corporation Ltd. (Energy Sector)
Sharad Sadadekar, HDFC Life Insurance Co. Ltd. (Insurance Sector)
Vishal Salvi, HDFC Bank Ltd. (Banking sector)

DSCI Excellence Award: Privacy Leader of the Year
Burgess Cooper, Vodafone India Ltd.

Law Enforcement Segment

DSCI Excellence Award: Capacity Building of Law Enforcement Agencies
Central Bureau of Investigation (CBI)

DSCI Excellence Award: India Cyber Cop of the Year
Suresh Kumar, Police Inspector, Cyber Crime Cell, Haryana, Gurgaon Police
9th Annual Information Security Summit 2014

2-4 Dec, Mumbai
DATA SECURITY COUNCIL OF INDIA (DSCI)
A NASSCOM® Initiative

Niryat Bhawan, 3rd Floor,
Rao Tula Ram Marg,
New Delhi - 110057
P: +91-11-26155070/71,
F: +91-11-26155070,
E: info@dsci.in, W: www.dsci.in