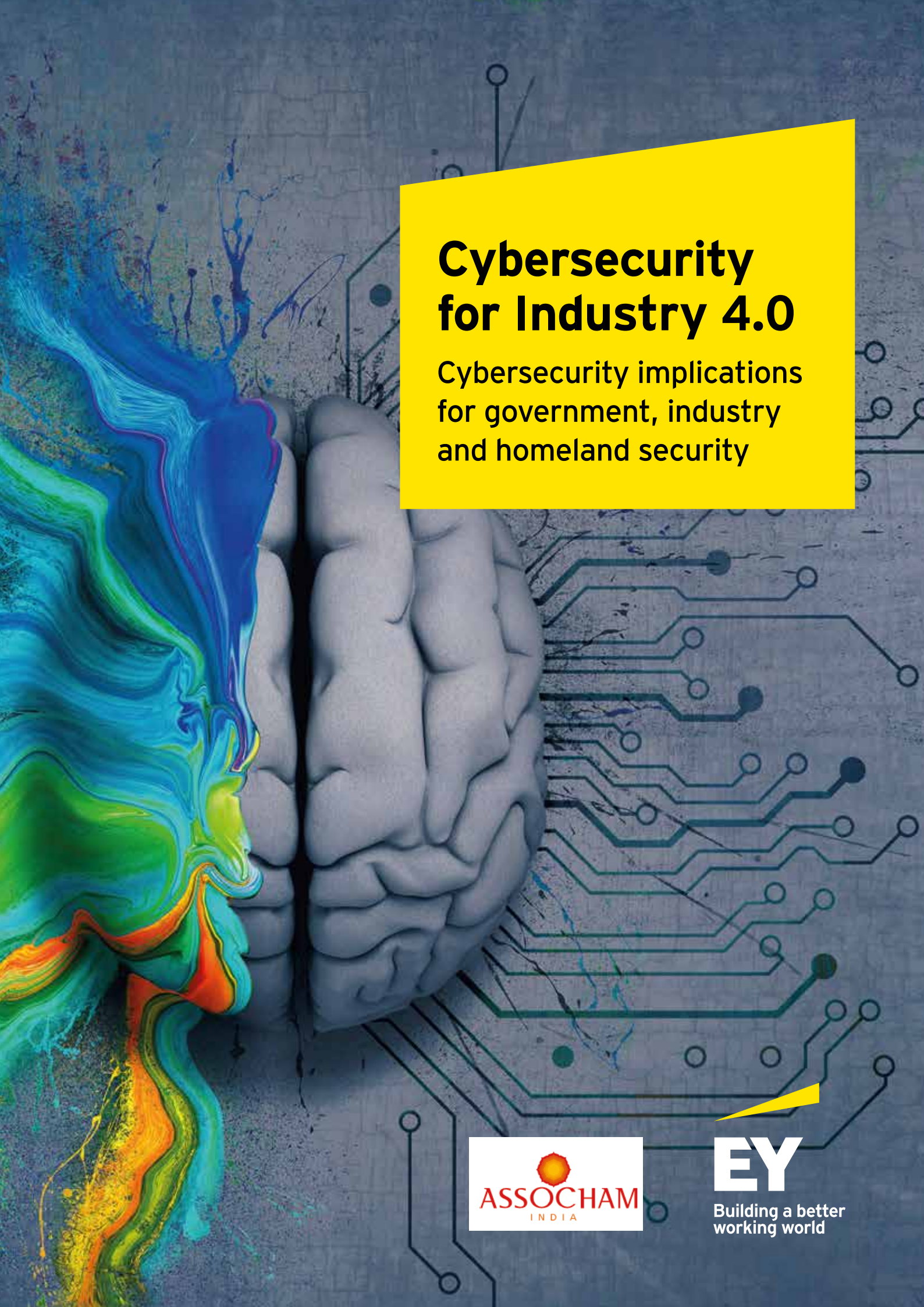


Cybersecurity for Industry 4.0

Cybersecurity implications for government, industry and homeland security

ASSOCHAM INDIA

EY
Building a better working world

Preface

In the realm of Digital India, where businesses, government and IT services are evolving from their traditional way of operations, emerging technologies in the current fourth industrial revolution will provide a further push towards providing better business solutions. Security and compliance in enhanced citizen services, optimized factory operations and improved healthcare facilities stand to directly see the light of day.

While deployment of cloud, big data, analytics, mobility and social media have helped businesses gain significant insights and improve services offered, Industry 4.0 "cyber-physical systems'" will further revolutionize the future way of work. Human augmentation technologies (such as Internet of Things, blockchain, Artificial Intelligence, robotics) will help streamline consumer engagement, behavioral design and regulation.

With the advent of newer technologies and collection, storing and processing of huge amounts of data, data security and privacy concerns are also on the rise. Especially in the context of the GDPR and the upcoming Personal Data Protection Bill in India, organizations need to change their methodology of data handling and have data governance frameworks in place to ensure compliance to these regulatory requirements.

India is well poised to reap benefits of Industry 4.0 technologies, however its input on and towards the Personal Data Protection Bill will need primary attention in order to ensure that security, regulatory and privacy concerns are addressed and all actions needed to strengthen the new industrial ecosystem.

Rahul Rishi
Partner & Leader – Advisory Services
(Digital Government)

ASSOCHAM

President's message

Security is an increasing challenge for individuals, institutions, businesses, and our nation. Security and peace are the prerequisite and essence of good governance for the civilized existence of a society. Be it internal security or securing the cyber space, they will be achievable only with everyone's cooperation, an intelligent policy and consistent practices.

As rightly said by our Hon'ble Prime Minister "...Security of the country is our priority. Internal security is our priority. Whether it is our oceans or borders, cyber world or space for all kind of security India is capable to defeat all such inimical forces....".

The Government of India is coming out with various schemes to curb this menace. We have to ensure perfect coordination and understanding between the various stakeholders to effectively execute these policies speedily.

ASSOCHAM is committed to creating more awareness about the National Security related issues and this whitepaper jointly prepared by EY and ASSOCHAM is a step in that direction, and we congratulate the team for their efforts.

We convey our very best for the success of the 11th India Security Summit 2018.

Sandeep Jajodia
President, ASSOCHAM

ASSOCHAM

Secretary General's message

India's internal security as also threat from outside remains a major area of concern. India is constantly facing growing challenges arising from cyber-crimes, physical crimes, economic frauds, insurgency, cross border developments etc.

With the advancement of technology, the criminals are now increasingly using sophisticated and innovative methods that require a constantly evolving response from the State. ASSOCHAM lauds the Government's pro-active efforts and while doing so emphasizes that interaction with the concerned stakeholders on ongoing basis is an urgent imperative.

We, at ASSOCHAM, have been discussing and deliberating with the concerned authorities and stakeholders about the need for security compliance and a legal system for effectively dealing with internal and external security threats.

ASSOCHAM is privileged to be a Member of the Joint Working Group (JWG) on Cyber Security set up by National Security Council Secretariat (NSCS), Government of India.

ASSOCHAM is committed to create more awareness about these issues and this Background Paper jointly prepared by EY and ASSOCHAM is a step in this direction. We congratulate the team for their efforts.

Our best wishes on this occasion for the success of the 11th India Security Summit with the hope that the Summit provides more insight into emerging security challenges and their appropriate solutions for further securing the Country from such crimes.

Uday Kumar Varma

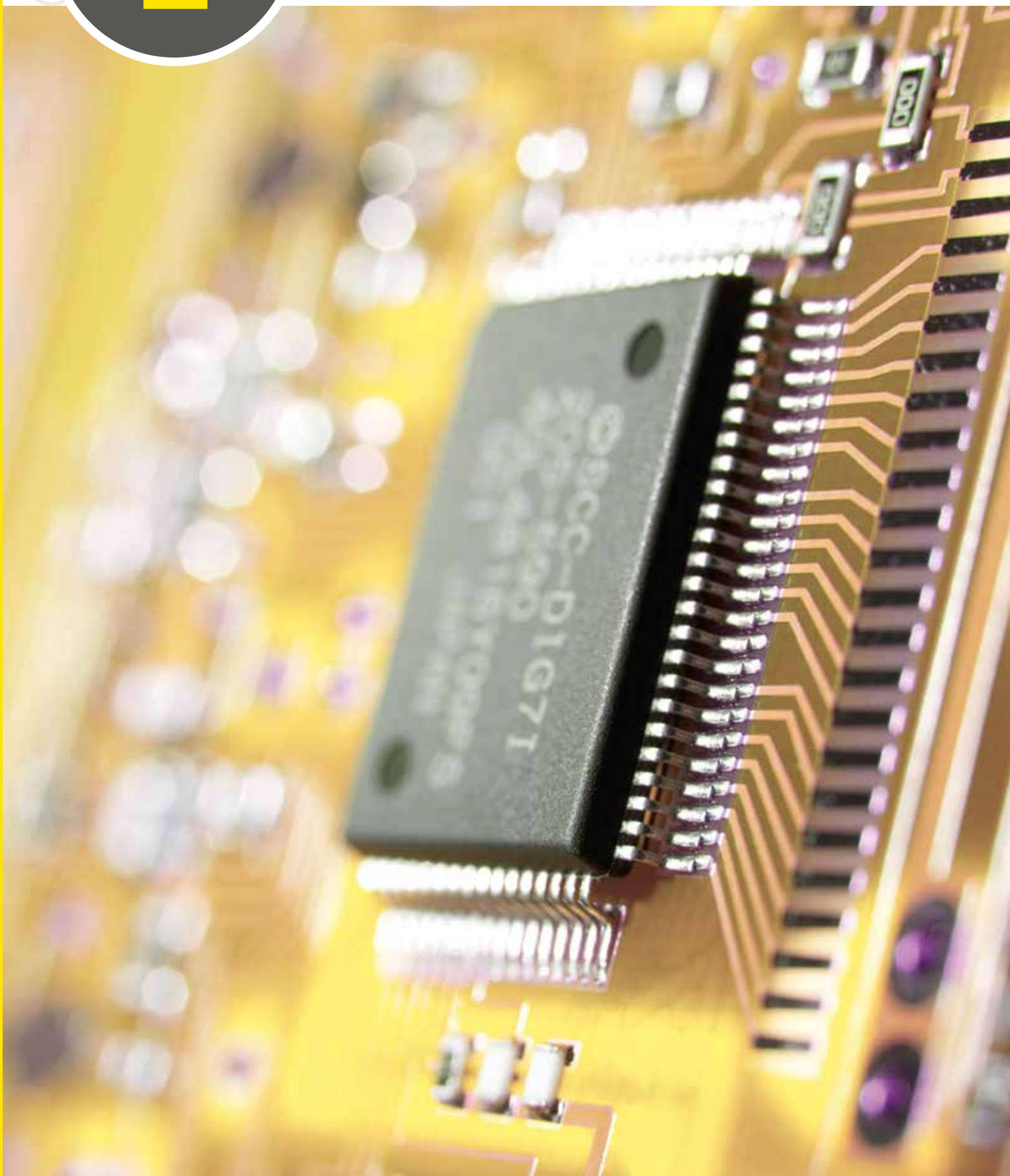
Uday Kumar Varma
Secretary General, ASSOCHAM

List of Abbreviations

Abbreviation	Definition
IP	Intellectual Property/ Internet Protocol
IoT	Internet of Things
AI	Artificial Intelligence
IT	Information Technology
CCTV	Closed Circuit Television
ANPR	Automatic Number Plate Recognition System
ITMS	Intelligent Transport Management System
PIS	Passenger Information System
DGCA	Directorate General of Civil Aviation
UAS	Unmanned Aircraft System
KYC	Know Your Customer
SSL	Secure Sockets Layer
DNS	Domain Name System
DDoS	Distributed Denial of Service
HIPPA	Health Insurance Portability and Accountability Act
ICRISAT	International Crop Research Institute for Semi-Arid Tropics
CPDM	Centre for Product Design and Manufacturing
ML	Machine Learning
NLP	Natural Language Processing
SOC	Security Operation Center
DLP	Data Loss Prevention
PII	Personally Identifiable Information

Content

1 Introduction



In an era which is being referred to as Industry 4.0, government departments are increasing their digital footprints and adapting their technology and engagement environments to remain competitive and relevant. As information and assets owned or used by the organization become another node in the network, the attack surface area increases exponentially. In such a scenario, the cybersecurity landscape is also undergoing a metamorphosis of unprecedented scale. Threats to homeland security are increasing due to various internal and external factors. Cybercrime has become more intense, sophisticated and potentially debilitating for homeland security. Technologies for Industry 4.0 will further intensify the need to upgrade measures for internal security. The challenges to security are becoming bigger than ever, with both sides– criminals and the defense – trying to remain ahead of each other. In today's hyper connected world, cyber-attacks are no longer a matter of "if", but rather "when".

It is impossible for an organization to prevent all attacks or breaches. Are we prepared for this?

Industry 4.0, with all its promise and vulnerabilities, is a reality. In this environment, organizations with well-crafted risk management and cyber security strategies are more likely to survive and succeed in the long term than those who do not address these with due care and due diligence.

What is Industry 4.0?

As computers and automation led the charge through the last few decades, companies, organizations and governments focused their efforts on revitalizing the IT infrastructure in the period also referred to as Industry 3.0. Today, however, the focus has shifted to technologies like Internet of Things (IoT), Artificial Intelligence (AI), blockchain, robotics, etc. which are defining the new work culture across almost all industries.

Industry 4.0 primarily merges automation with advanced manufacturing to reduce direct human effort and resources. Effectively, these technologies make the manufacturing system a "smart networked factory", where all activities are digitally controlled and are thus, immutable.

As a result, utilization of resources, both financial and material, is more efficient.

Industry 4.0 (I 4.0) can be the catalyst of changes in different fields like governance, management and administration of smart cities and other applications which are driving the vision of Digital India. Examples of such centers of innovation include the IIT Delhi and Mumbai Centers for Smart Manufacturing and another center at the Central Manufacturing Technology Institute, Bengaluru. Capacity building for I4.0 is carried out by the SL Kirloskar Centre of Excellence for IoT.

With so much dependence on data flow and communication between processes, components and sub-systems, data integrity and systems integrity assume critical dimensions. Manual supervision of various processes is neither feasible nor effective. Even patching security flaws from time to time is not practical – data by itself needs to be both abstracted and secured through different tools and techniques. Following secure design principles and guidelines such as in ISO 21827 is critical to secured system design.

Securing Industry 4.0 requires a de-novo approach which is explained in next section.

Only

4%

of organizations are confident that they have fully considered the information security implications of their current strategy, and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks.

Figure 1: Progression of Industrial Revolution

Industry 3.0	Industry 4.0	Industry 5.0
▶ Computers	▶ Automated physical systems	▶ Industrial robots
▶ Automation	▶ Smart Cities	▶ No direct interaction
▶ Last mile access	▶ Internet of Things	▶ Mechanical Replication
▶ Digital procurement and sales	▶ Robotics	
	▶ Blockchain	

Cybersecurity for and through Industry 4.0

In first few years of this millennium, cybersecurity was more about protecting people and organizations from traditional threats such as malware, social engineering attacks, website defacing, hacktivism, etc. Last few years have witnessed increased sophistication and intensity in cyber-attacks, which are now oriented towards financial crime, industrial espionage and have even targeted governments and critical infrastructure from time to time.

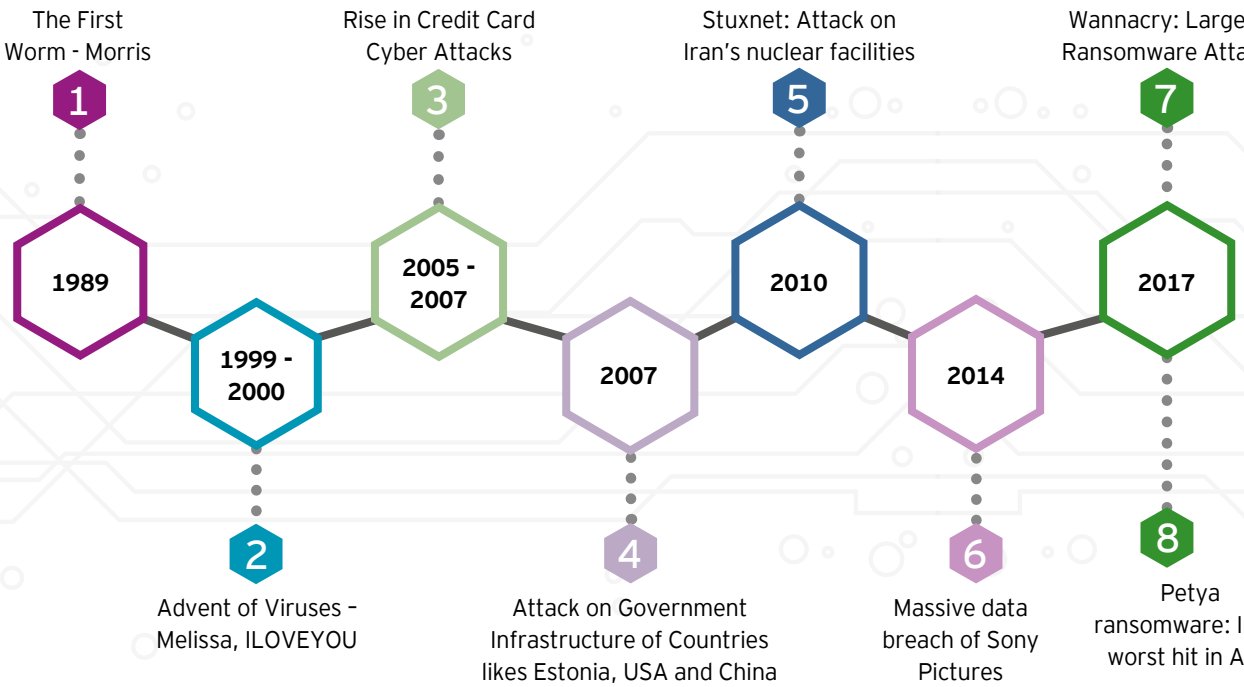
In era of Industry 4.0, the organizations are hyper connected with their smart devices and smart networks. This presents a very lucrative target for the cyber criminals who find many more easy and insecure entry points into networks and devices. Botnets[1] have become the weapons of choice to carry out DDoS and crypto-jacking attacks. Cyber-attacks on critical infrastructure and strategic industrial sectors have become more frequent and sophisticated. These not only cause disruption in the normal functioning of societies[2] but have crippling effect on the morale and psyche of the victim countries. Ukraine has unfortunately faced the brunt of multiple such attacks on their energy grid, forcing blackouts in some regions[3] . In the US, attacks on the energy grid are attempted on a daily basis, but strong cyber security mechanisms have ensured that minimal damage is inflicted.

As new threats, techniques and attack vectors emerge, the focus of cybersecurity is slowly but surely shifting away from classic perimeter based approach to a 360 degree orientation.

This is required to protect hyper-connected systems, network and data of this generation from damages and unauthorized access. This is accepted by the CEOs of Fortune 500 companies, who identify the pace of technological change and cybersecurity[4] as the biggest challenges they face today.

Cybersecurity should no longer be viewed as a function of information technology or information security alone. It needs to form an integral part of culture and strategy of the organization. It should be reflected in each and every facet of the organization, right from the strategy to the behavior of an individual employee. Such an integrated cybersecurity vision aligns business functions of the organizations with needs of the stakeholders and becomes a more acceptable strategy.

Figure 2: History of cyber attacks



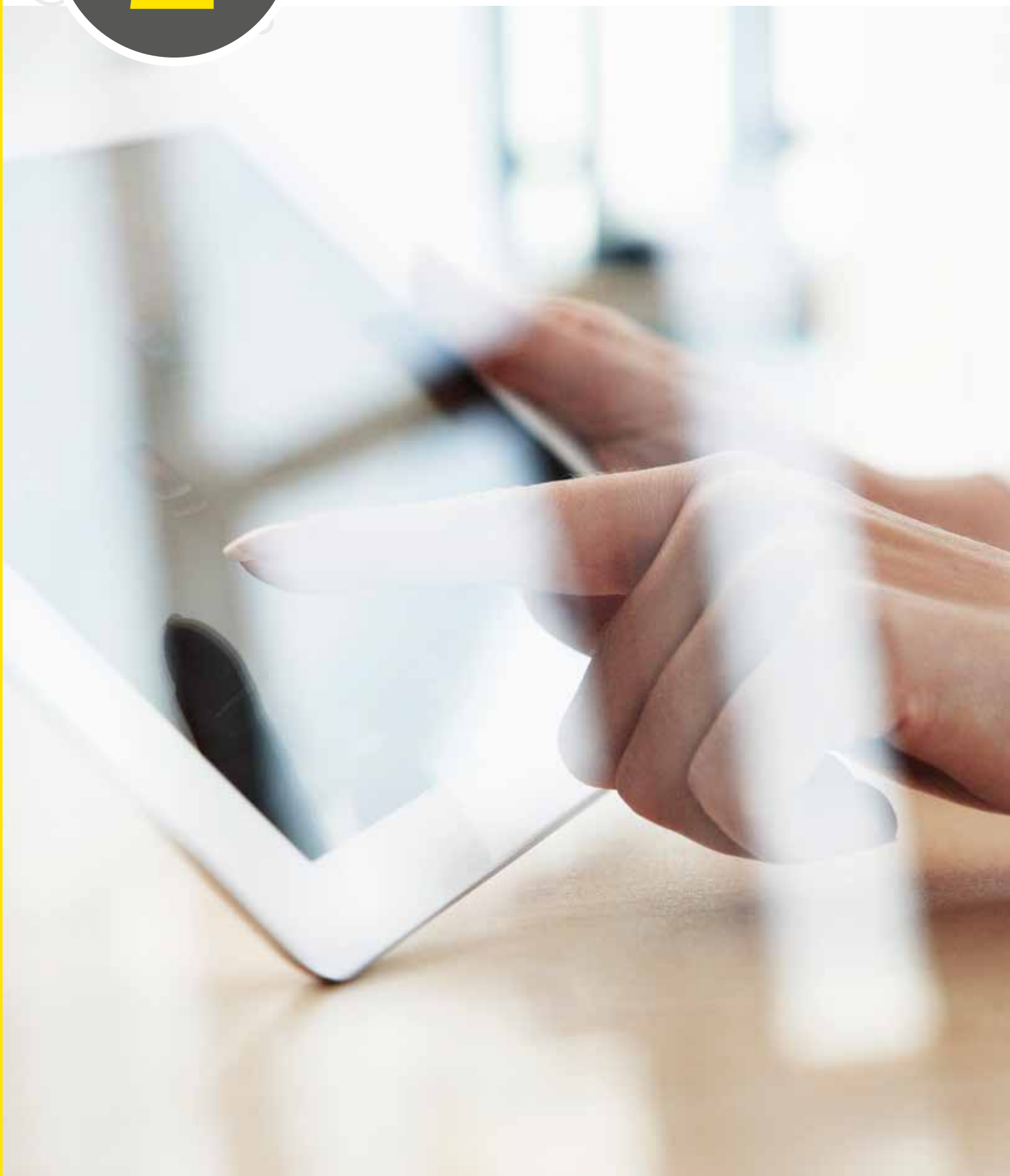
[1]Kolias, Constantinos & Kambourakis, Georgios & Stavrou, Angelos & Voas, Jeffrey. (2017). DDoS in the IoT: Mirai and other botnets. Computer. 50. 80-84. 10.1109/MC.2017.201.
[2]"Global Risks Report 2018", World Economic Forum
[3]https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/russian-hackers-attack-ukraine/amp
[4]http://fortune.com/2017/06/08/fortune-500-ceos-survey-ai/

> Putting cybersecurity at the heart of an organization´s strategy will help maintain and even enhance the trust of consumers, regulators and the media

All survey statistics in this report refer to EY's Global Information Security Survey 2017 – 2018 "Cybersecurity regained: preparing to face cyber-attacks".
For further information, please access:
https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

2 Internet of Things

When things are hyperconnected



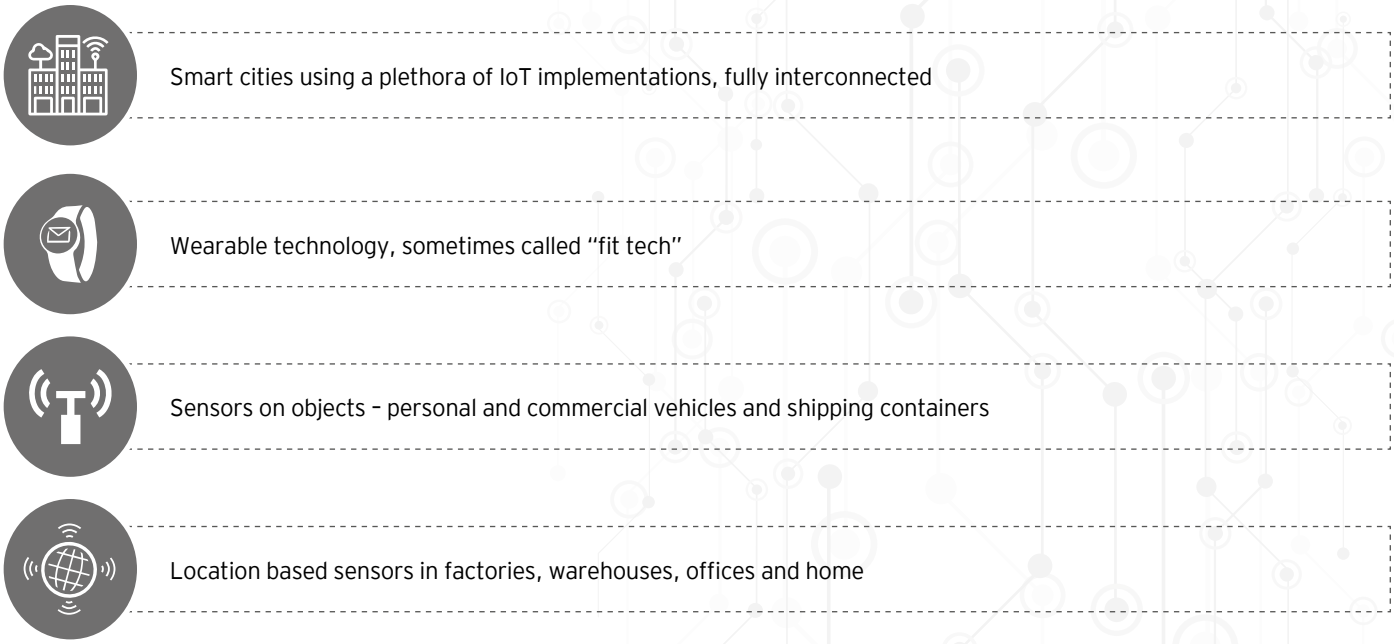
The IoT phenomenon is one of the most disruptive technologies changing the way organizations function and carry out business. It is a system of inter connected computing devices, mechanical and digital machines, objects or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Devices and sensors are used to collect data from everywhere – home, cars, office, manufacturing plant, hospital, etc. The data is collected and processed to automate responses or provide tools for decision making. IoT is aimed at increasing efficiency and productivity while conserving resources.

Government of India is developing 100 smart cities where IoT will be used in the applications listed below[5]:

- Smart parking
- Tele-care
- Intelligent transport system
- Citizen safety
- Smart urban lighting
- Smart grid
- Waste management
- Smart energy
- Smart city maintenance
- Water management

IoT relies on effective connectivity across land, air and water. Robotics and drones, therefore, are essential building blocks of an IoT ecosystem, in many ways, elaborated below.

Figure 3: Use cases of IoT technology



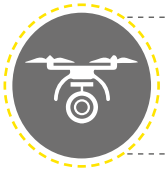
[5]https://www.mygov.in/sites/default/files/master_image/Revised-Draft-IoT-Policy-2.pdf

Success of smart cities hinges on real time surveillance and monitoring.

Drones can prove to be really effective in this field. Drones can act as rapid deployment solutions for surveillance, crowd monitoring, etc. in areas which have restricted space for movement and for search and rescue missions. Drones could have been effectively used in Kerala, during the recent floods, for reconaissance, supply drops, aerial photography and measurement of geological metrics if there was a proper policy in place for such eventualities. Directorate General of Civil Aviation (DGCA) has released draft of guidelines for Unmanned Aircraft System (UAS) to streamline the adoption of the technology in India. Law enforcement and disaster response agencies will be able to deploy drones to reinforce their capabilities.

Figure 4: Use cases of drones

Provides real time aerial traffic monitoring. The gathered data can be used for analysis and provide forecasting and solutions to control traffic.



Drones offer a quick and immediate aid for out of reach zones. Deployable in unfriendly climatic conditions they provide help to crisis responders by distinguishing dangers and spotting casualties

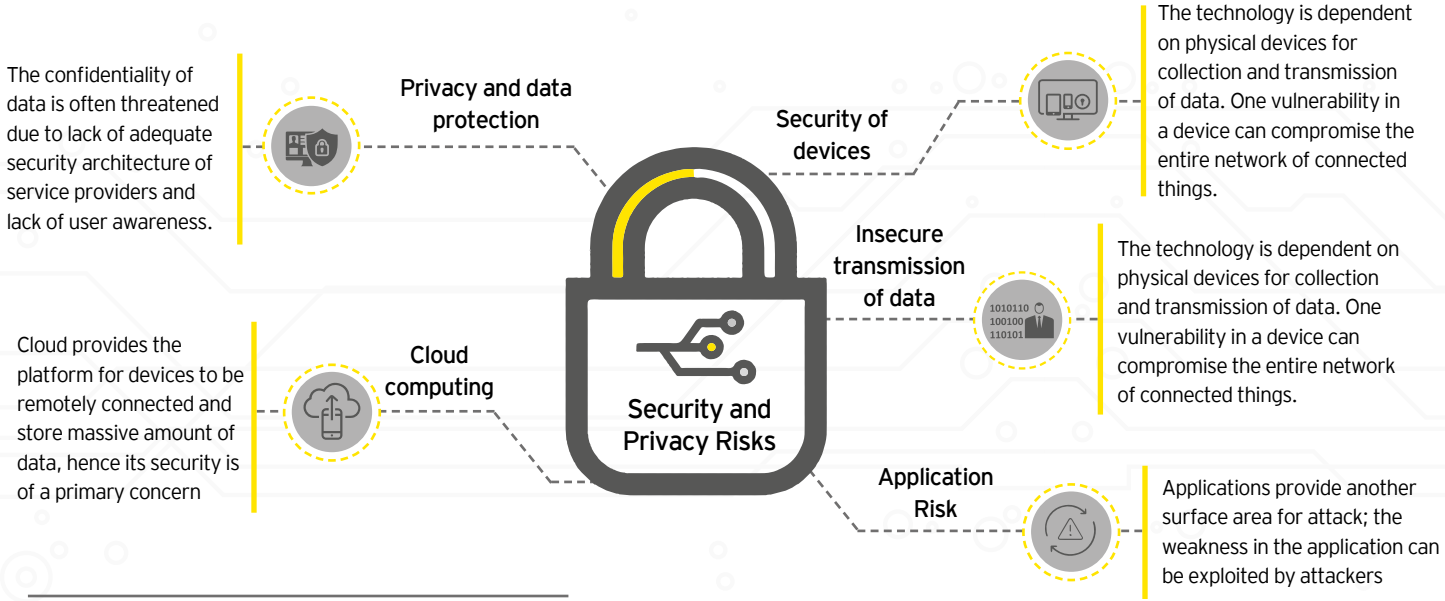
Aids in monitoring the battle regions, and conduct scans for lost or harmed military officers.

Security and privacy risks

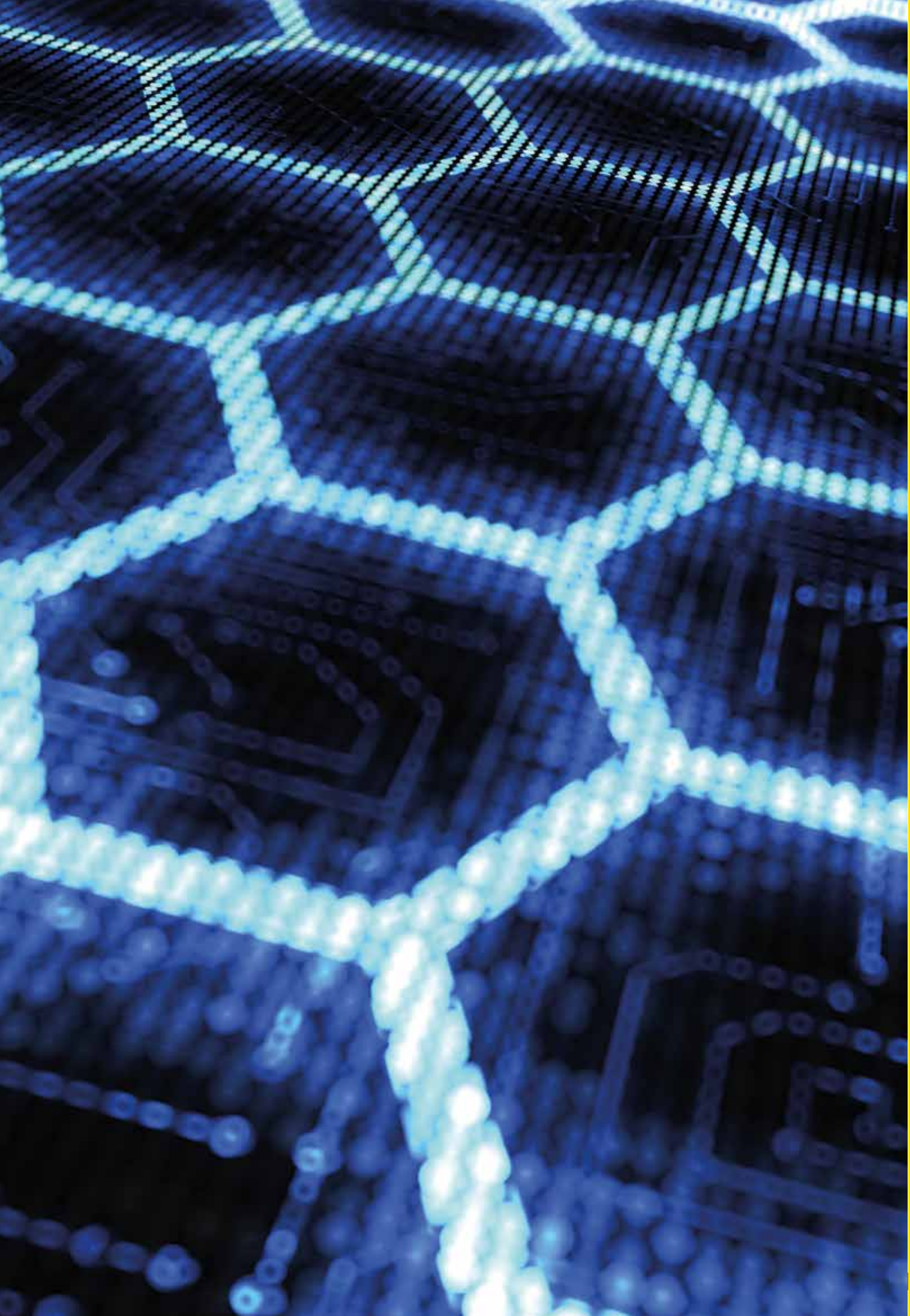
Estimates have been made that internet-connected things will outnumber humans 4-to-1[6]. Even if a few of these devices are not secured properly, cyber criminals will have easy access in to the IoT network and would be able to disrupt the services.

Security by design is an approach to software and hardware development where security is built in from the beginning, and not as a late addition after a hacking incident. The need for security by design has become crucial as tech companies continue to churn out a myriad of IoT objects for consumers and enterprises. Most of these objects were designed with no security built into their system, making them easy targets for security breaches.

Figure 5: Security and privacy risks of IoT



[6]https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf



3 Blockchain

When things are decentralized

Blockchain as a concept has been around for nearly a decade. It is a well understood and defined concept that forms the backbone of the most used crypto currency. Blockchain, as a technology, focusses on integrity and immutability of transactions.

The blockchain development space is exciting- worldwide corporate spending on blockchain solutions is forecasted to double and reach nearly US$2.1 billion in 2018 compared to last year, according to the "Worldwide Semiannual Blockchain Spending Guide". By 2021, investment is expected to reach US$9.7 billion.

Blockchain promises to:

- Increase the speed, the efficiency and the security of transactions and ownership transfers of digital assets
- Remove bottlenecks, a phenomenon associated with central servers
- Eliminate the need for central authorities to certify ownership and clear transactions
- Reduce fraud and corruption by providing a transparent public and auditable ledger
- Reduce administrative cost using agreements that can automatically activate secure and trusted actions based on specific conditions (smart contracts)

In context to IoT and its applications, blockchains can be used to ensure data integrity and security, seen in projects like Atonomi which focuses on a security protocol, IBM Watson IoT integrated with blockchains and startups like IOTA that aim to be an underlying technology for IoT applications.

Keyless Signature Structure is a block chain based technology which is helping the Estonian government create a verifiable security system[7]. It replaces the traditional key based data authentication by storing hashes of original files, data on the block chain. By using hashing algorithms, they are able to compare and verify other copies of information stored in the other nodes, allowing easy discovery of data tampering and alterations.

While blockchain as a technology is still niche and growing, it presents solutions that current centralized offerings can compete in terms of speed but not capacity and trust. Inherently, in IoT, blockchains will be used to secure infrastructure while maintaining device interoperability.

Figure 6: Blockchain

Blockchain is a distributed infrastructure technology - it is a decentralized ledger that keeps a record of each transaction that occurs across a network which enables a decentralized exchange of trusted data – a 'shared record book

Distributed Ledger:

- Every participant in the network keeps a copy of all the transactions.
- Transactions are secured by encryption to prevent tampering.

Consensus Algorithm:

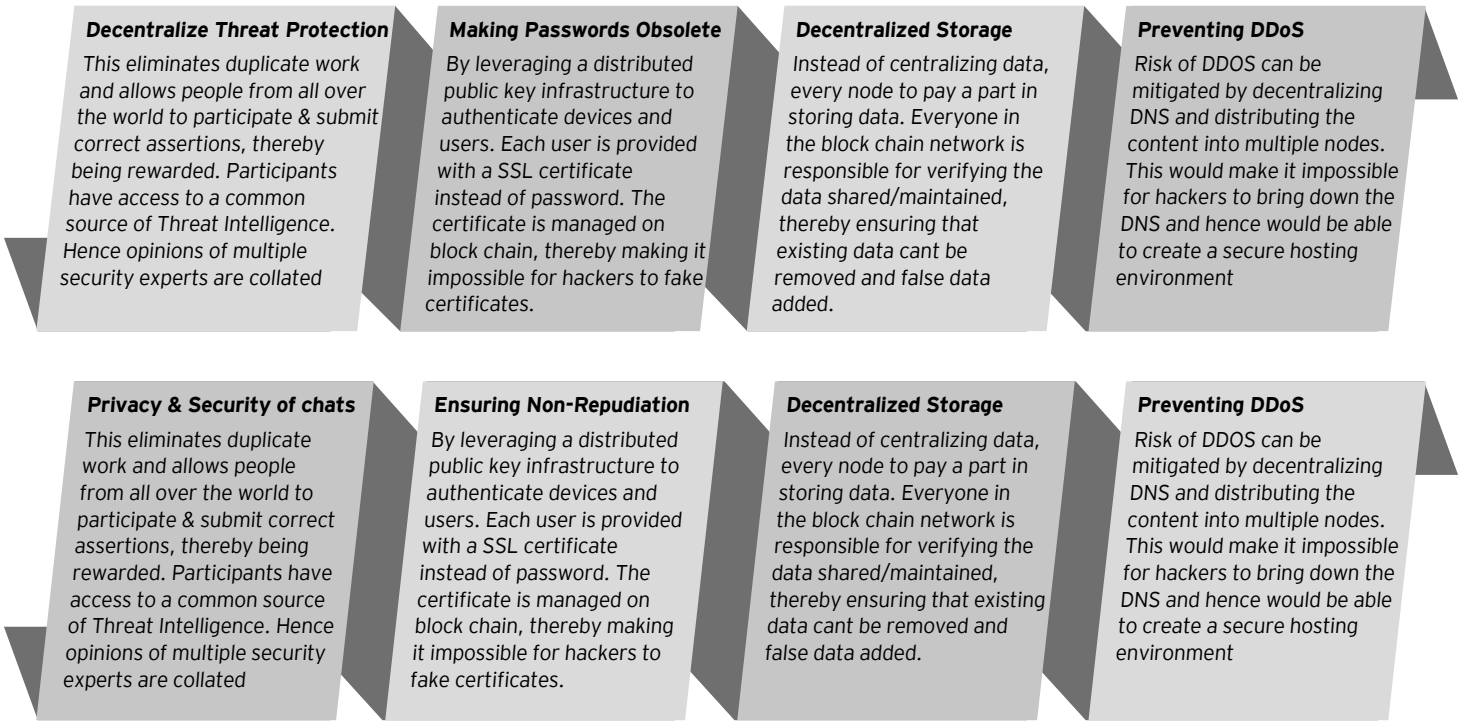
- No one node or server is responsible for approving transactions leading to genuinely distributed
- Each entry validated and recorded on all ledgers across network

Smart Contracts / Programmable Ledger:

- Transactions can be sent with rules attached - small programs that govern when and how transactions are processed.

[7]https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

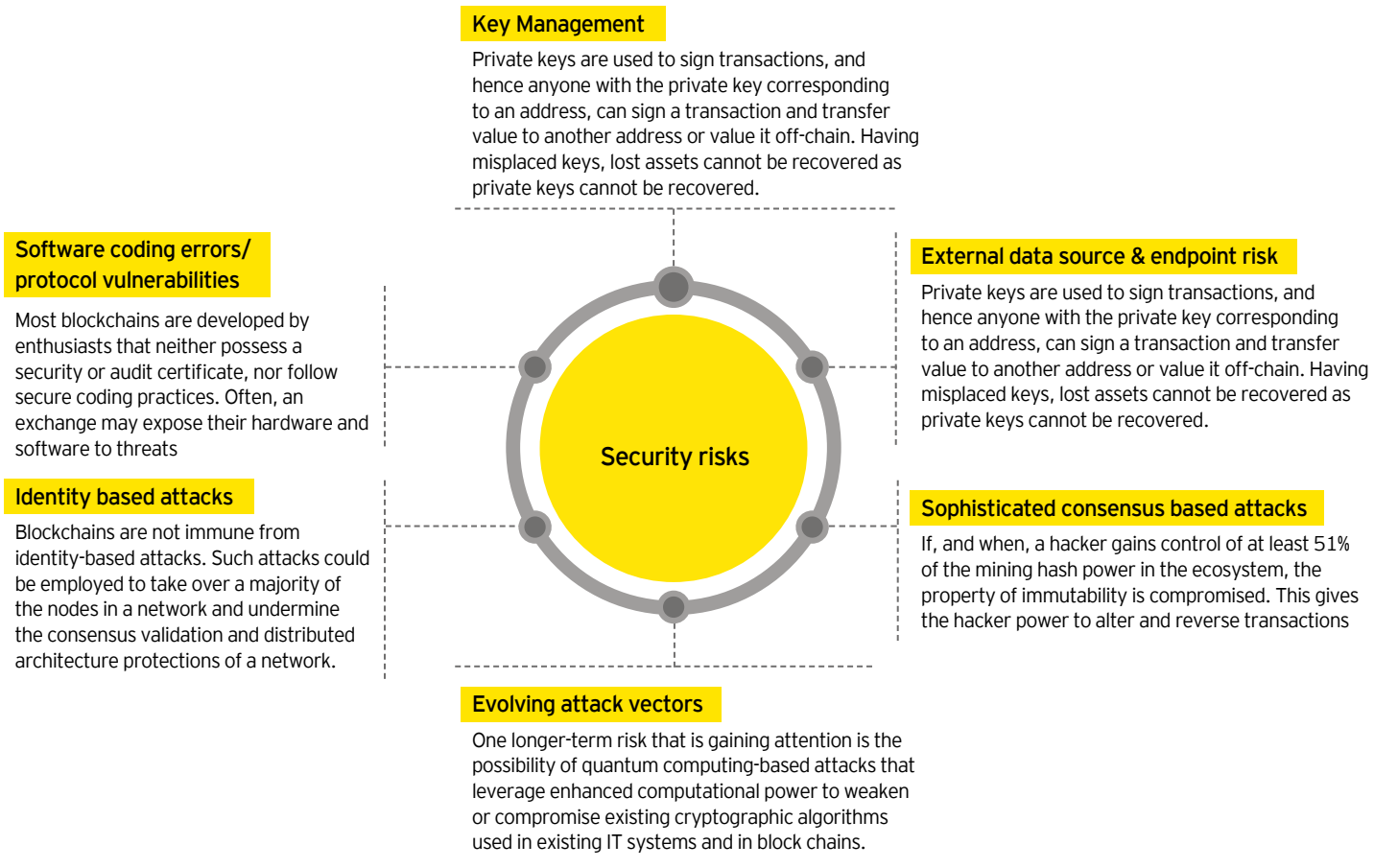
Figure 7: Blockchain use cases



Security risks

Although Blockchain holds immense promise and potential, it remains vulnerable to cyber threats and risks. A robust cybersecurity program is therefore imperative for protecting blockchain assets from cyber threats shown in the figure below.

Figure 8: Security risks of blockchain



Privacy risks

Transactions in a public blockchain network are globally published and if someone gets access to public keys/wallet ids, they would be able to view all the transactions. This leads to a larger privacy concern in public block chain networks.

As per proposed data privacy laws in India and elsewhere like EU, data principals can exercise the right to be forgotten and data erasure, which is a challenge in a blockchain environment, given its immutable nature.

In a public blockchain, every node of the network stores data and the same is publicly accessible to anyone, regardless of the original purpose of the data collection and processing, thereby violating the principles of data privacy.

Although blockchain and data privacy principles are seemingly contradictory in scope, they have some principles in common. Members of the platform could enter information and have their own copy of the ledger instead of the data being stored centrally. This also supports HIPAA principles because, having multiple checkpoints – allows patients to have more control in their data and be able to approve/reject any sharing/modification of their data.

A shared Know Your Customer (KYC) network allows banks and institutions to share KYC information between them over the network, a customer can share his/her personal data once with the bank, then when acquiring products or services from another institution, give consent to the network to provide the KYC evidence to the other institution.

Why is blockchain important for homeland security?

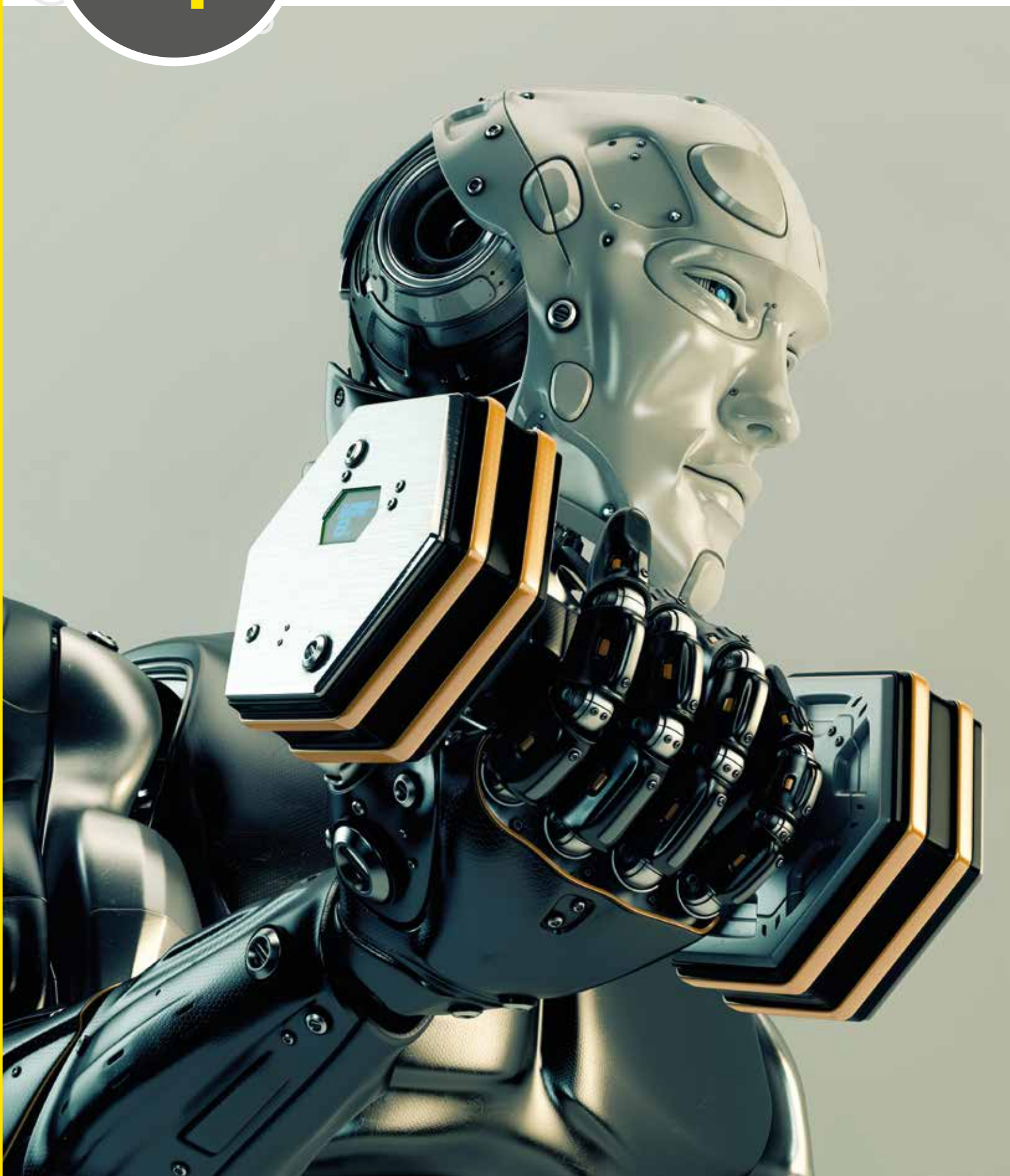
Blockchain will enable a wider variety of transactions, such as collecting taxes, delivering benefits, issuing documents and recording properties. Governments can use blockchain in sectors such as public safety, social services and identity management.

Andhra Pradesh is slated to become the first state in India to adopt blockchain for governance. It has piloted two key projects: **managing land records** and **streamlining vehicle registrations**[8]

[8]https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/#7ced7768f562

4 Artificial Intelligence

When things are intelligent



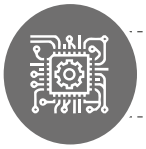
[9]Artificial Intelligence (AI) is another technology that has started impacting government departments and internal organizations in a major way. It is an area of computer science that helps building solutions with human like intelligence and can carry out complex tasks independently. AI applications are based on neural networks, machine learning, deep learning and Natural Language Processing algorithms. Machines act like humans only after they are trained well to accomplish specific activities by processing huge amounts of data and identifying patterns in it. The growing interest and value proposition of the technology is resulting in IT companies/software vendors to include AI in most of their service propositions[12].

Gartner predicts that global Artificial Intelligence business value will reach US $1.2 trillion by 2018 and by 2020, AI will create more jobs than it eliminates.

Major initiatives in the field of AI have been taken by Google, Apple, Amazon and others. Government of India has appreciated the immense potential of AI and has made significant investments to use it for better governance and service delivery as illustrated below:

Figure 9: Initiatives by Indian Government in the field of AI

PM Narendra Modi Government has set up an AI task force, appointed by Ministry of Commerce and Industry in order to prepare India for the upcoming Industrial Revolution 4.0 through a Public-Private Partnership



The AI Task Force of the Ministry of Defence has shared their final report on how AI can aid in gaining military superiority and the strategic implications of AI from a National Security Perspective

Niti Ayog has come up with India's strategy on AI for the development of the following sectors on focus: health care, agriculture, education, smart cities and infrastructure, and smart mobility and transformation

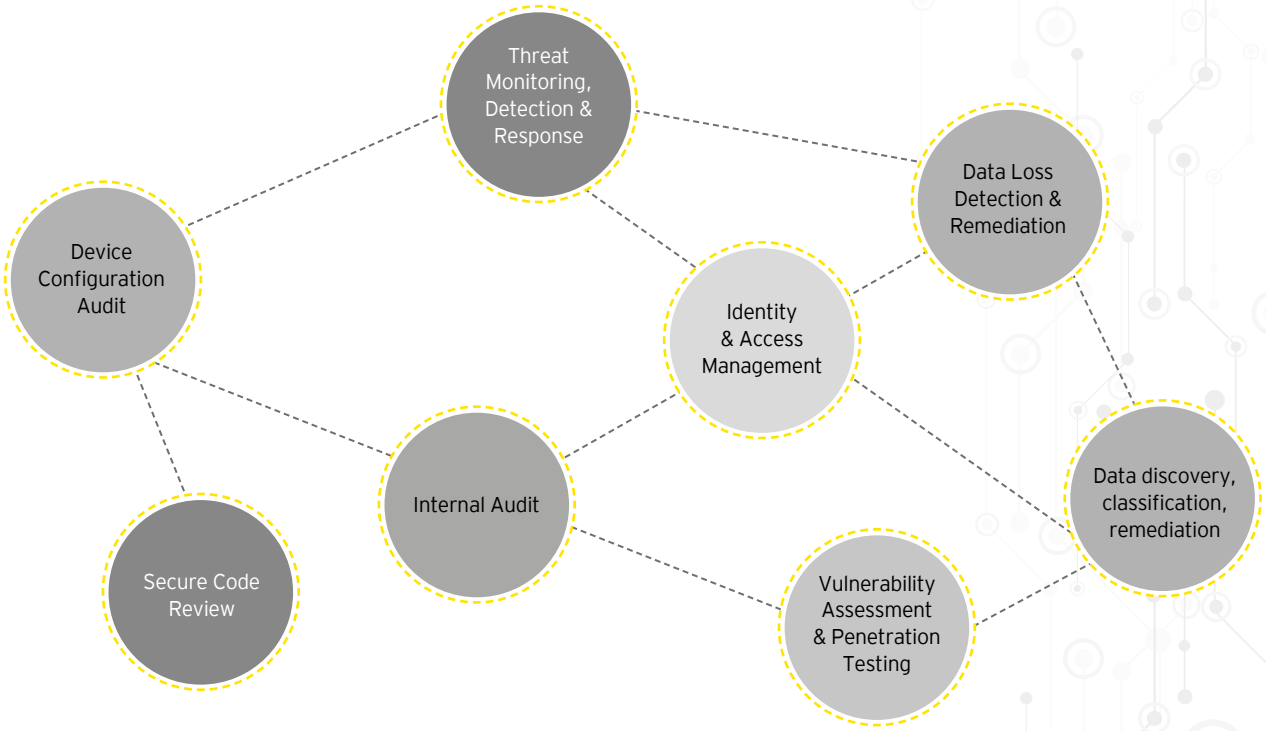
> **New and emerging technologies like Artificial Intelligence and Robotics are perhaps the most important determinants/ of defensive and offensive capabilities for any defence force in the future. India, with its leadership in Information Technology domain, would strive to use this technology tilt to its advantage[10].**
>
> Prime Minister Narendra Modi
> DefExpo 2018, Chennai

[9]https://timesofindia.indiatimes.com/india/india-moves-to-develop-ai-based-military-systems/articleshow/64250232.cms
[10]https://www.narendramodi.in/pm-modi-inaugurates-defexpo-2018-in-mahabalipuram-539632

AI in the field of cybersecurity

AI has the potential to make cybersecurity more efficient and responsive against ever increasing threats and improve the cyber security posture of an organization. Some of the cyber security areas which are amenable to AI are described below:

Figure 10: Application of AI in cybersecurity



Threat monitoring, detection and response:

AI and Machine Learning (ML) allow the systems to monitor a wider range of evolving threat vectors (rather than monitoring threats against previously identified signatures). Machine learning can track anomalous behavior easily and help in predictive analysis of threats and attacks. Complex analytics using historical data combined with clustering, clipping, data visualization etc. can be carried out without human intervention and allow security administrators to respond in near real time to security events and incidents. This will take threat detection and alert generation to the next level.

Audit:

ML can increase efficiency of configuration management, configuration audit and cyber security audits by removing human errors and biases. These solutions can enhance the performance and reduce the risk in internal audits by reviewing a larger data set (for E.g.: evaluating all transactions of a year) as compared to evaluating a representative sample as done in conventional internal audits against known internal control red flags, thereby ensuring audit completeness and quality reports.

Secure code review:

NLP techniques (Natural Language Processing algorithms) are utilized in automated code review for better detection and reporting of bad coding practices or security vulnerabilities. Automating code reviews can help reduce costs, ensure code health and increase productivity by focusing on the most harmful vulnerabilities.

Access management and network monitoring:

Access management is another area where AI and ML can increase efficiency and effectiveness. Cyber security of systems, applications and data bases can be improved through continuous learning and updation of rules. They can also aid in monitoring network traffic and identifying any abnormal activity and raising alarms or taking pre-emptive actions to block any traffic which can harm the networks or applications, thereby integrating the functionalities provided by multiple security tools in a SOC.

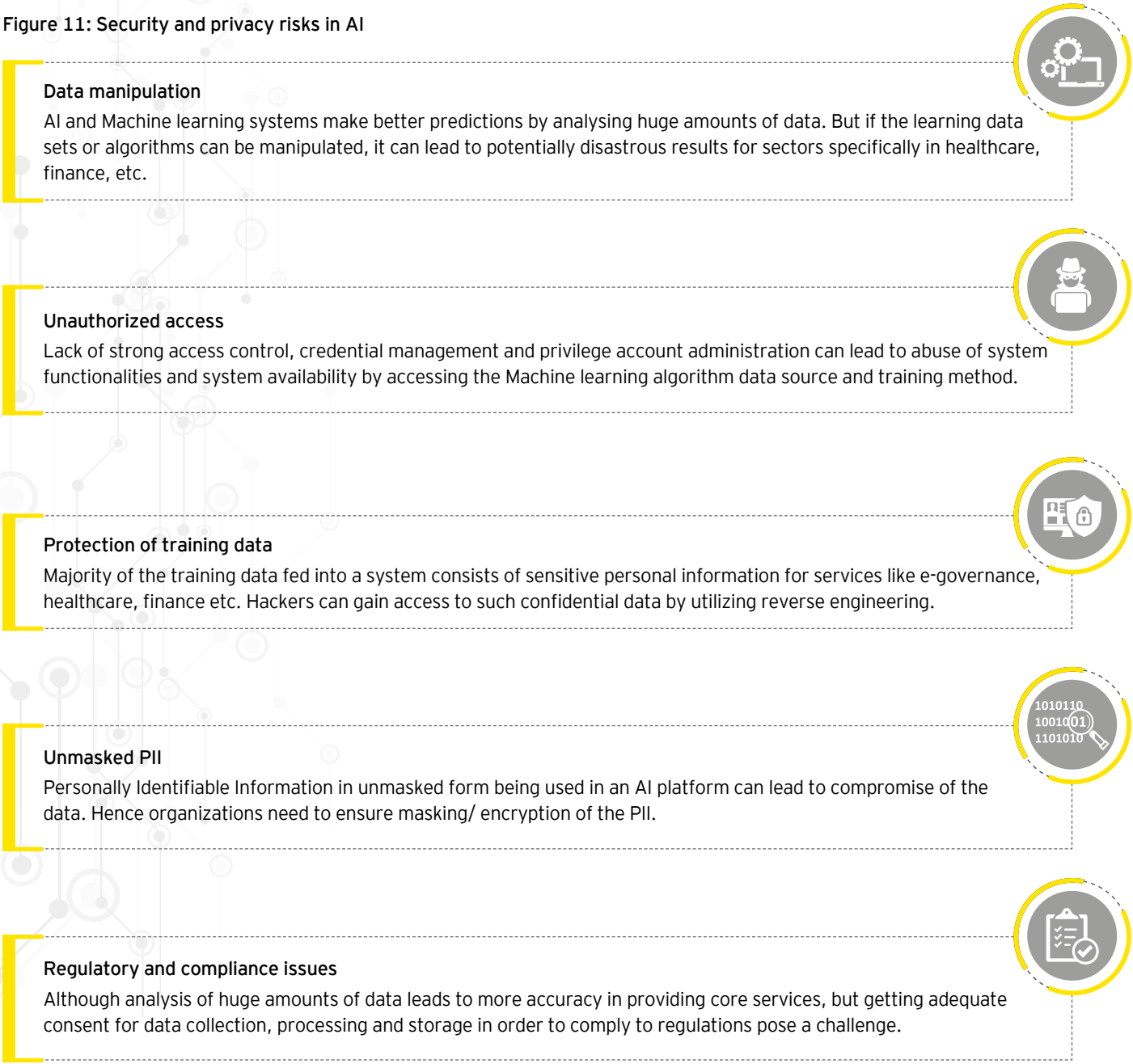
Data discovery, classification and loss detection/prevention:

ML techniques can be used to enhance offerings by typical Data Loss Prevention (DLP) solutions by automating classification, monitoring and prevention of sensitive data loss by using predictive models to identify sensitive personal or health or financial information and tracking access patterns to these data sets from new/unusual activity from existing sources.

Vulnerability assessment and penetration testing:

AI based vulnerability scanning applications are able to crawl dynamic pages, detect vulnerabilities which otherwise require human intelligence, thereby reducing cost and increasing efficiency and reducing false positives.

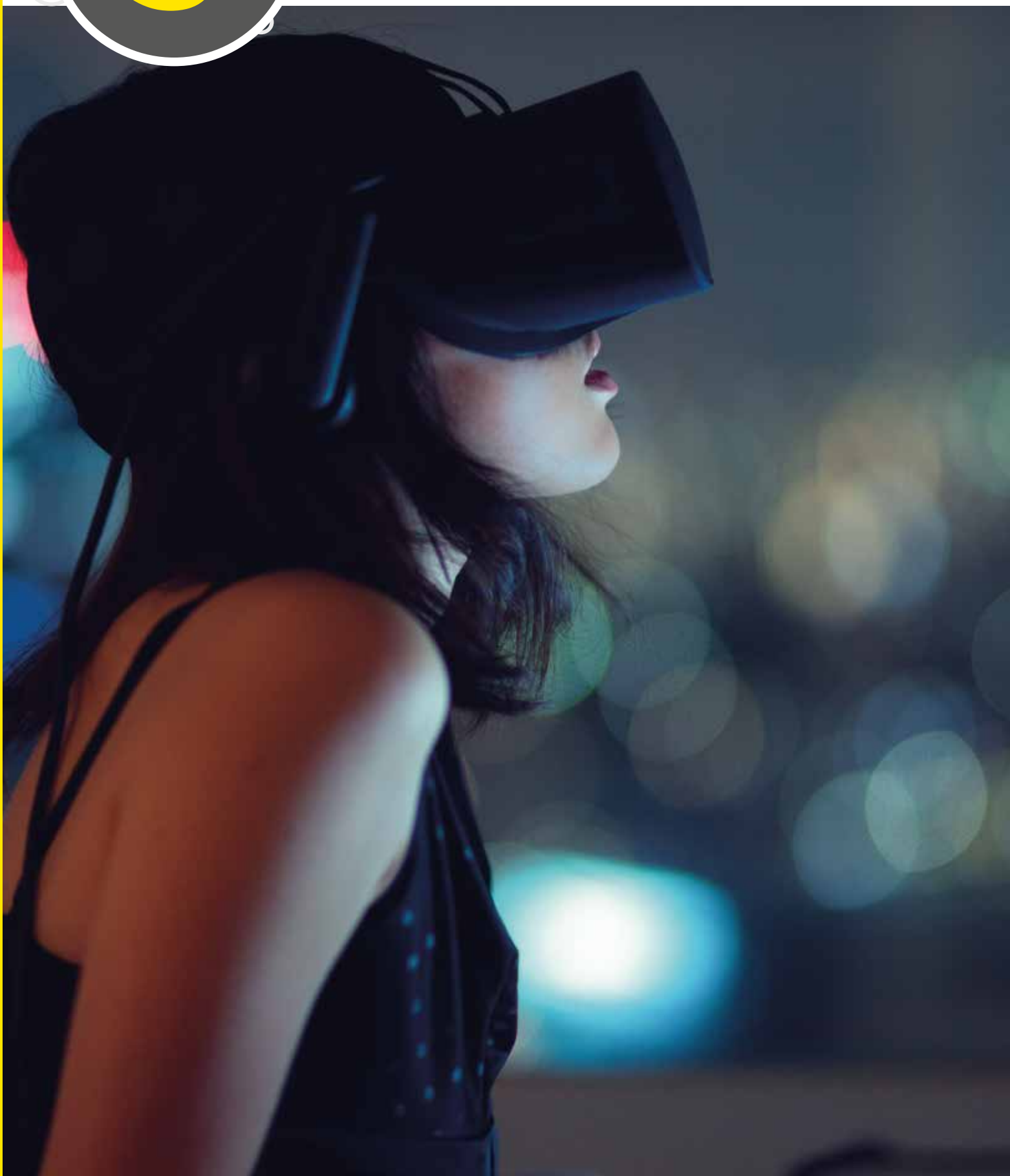
Figure 11: Security and privacy risks in AI



Why is AI important for homeland security?

AI will drive significant changes in the way governments work and serve their citizens, especially from a homeland security perspective. AI-based applications could potentially reduce backlogs, cut costs, overcome resource constraints, free workers from mundane tasks, improve the accuracy of projections, inject intelligence into scores of processes and systems and handle many other tasks humans can't easily do on our own, such as predicting fraudulent transactions, identifying criminal suspects via facial recognition and sifting through millions of documents in real time for the most relevant content.

5 Way forward



According to Gartner's Hype Cycle of Emerging Technologies, IoT, Blockchain and AI have not yet attained their optimum potential and are likely to mature in next few years. As explained earlier, these can be effectively used to improve consultancy, governance and overall digitalization of major industries. Adoption of these technologies will enhance the operational capability, talent acquisition and application delivery across different sectors and organizations.

Along with opportunities, every new technology brings risks. It is imperative for organizations to fully understand the implications before adopting these technologies for cyber security. In order to achieve actual benefits of the fourth industrial revolution, the government will need to take measures so that the cybersecurity market in India grows hand in hand with the Industry 4.0 market. Sector specific security baselines and an integrated data protection framework will help India to derive sustainable benefits from the current technological revolution. Government and organizations face a challenge to be cyber resilient in order to adapt to evolving and disrupting technologies. Traditional information security practices might provide necessary approach but might not be enough to completely protect the organizations.

Organizations need to focus and commit to a framework that:

- Provides an integrated approach to cybersecurity – holistic approach to threat landscape rather than employing security technologies in silos
- Develops capabilities for threat detection to respond appropriately and proactively
- Employs the use of AI to recognize patterns for smart monitoring of the IT infrastructure
- Develops strong relationships between organizations across different sectors and government bodies for sharing information, intelligence, capacity building and research

As these technologies develop and scale up, education and inclusion of human resources become the cornerstone for their progress. Successful adaption of these technologies require new skills. In Industry 4.0 and its emerging technologies, gender diversity, cultural diversity and *divyangjan*, or differently abled bodies inclusion form a core of human resource management and merit based recruitment. Empowering and disinhibiting these is a fundamental aspect of innovation in governmental departments and organisations. A simple D&I strategy may cover the following[11]:

- Creating proactive, high performing teams through capacity building with D&I principles guiding the entire process
- Introducing these teams to vendors, consultancies and other departments for greater interoperability
- Making office spaces more inclusive for *divyangjan* or differently abled, with an accessibility-oriented focus
- Equipping managers and team leaders with skills to lead inclusively
- Establishing mutual accountability for equitable development, sponsorship

Capacity building in human resources for Industry 4.0 must involve a multi-pronged strategy internally in departments, with a ground-up focus on mindset development. It is important for the government to develop programs for skill upgradation of existing man-force and ensure that the curriculum of school and universities is suitably modified to include these as core subjects in future. End users also need to use these with due care so that they derive desired benefits without becoming vulnerable to security and privacy risks.

> **In the Fourth Industrial Revolution, talent will become more important than money.**
>
> **Shri Narendra Modi**
> *Hon'ble Prime Minister*

[11]https://www.ey.com/Publication/vwLUAssets/EY-our-approach-to-diversity-and-inclusiveness/$FILE/EY-our-approach-to-diversity-and-inclusiveness.pdf

References

1. https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf
2. https://www.gartner.com/newsroom/id/3872933
3. https://www.gartner.com/newsroom/id/3837763
4. https://searchmobilecomputing.techtarget.com/news/450419686/Artificial-intelligence-data-privacy-issues-on-the-rise
5. https://cis-india.org/internet-governance/files/AIManufacturingandServices_Report_02.pdf
6. https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/#5a9f62188f56
7. http://houseofbots.com/news-detail/2747-1-ai-chatbots-transforming-the-indian-banking-industry
8. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

ASSOCHAM

The knowledge architect of corporate india

Evolution of Value Creator

ASSOCHAM initiated its endeavour of value creation for Indian industry in 1920. Having in its fold more than 400 Chambers and Trade Associations, and serving more than 4,50,000 members from all over India. It has witnessed upswings as well as upheavals of Indian Economy, and contributed significantly by playing a catalytic role in shaping up the Trade, Commerce and Industrial environment of the country.

Today, ASSOCHAM has emerged as the fountainhead of Knowledge for Indian industry, which is all set to redefine the dynamics of growth and development in the technology driven cyber age of 'Knowledge Based Economy'.

ASSOCHAM is seen as a forceful, proactive, forward looking institution equipping itself to meet the aspirations of corporate India in the new world of business. ASSOCHAM is working towards creating a conducive environment of India business to compete globally.

ASSOCHAM derives its strength from its Promoter Chambers and other Industry/Regional Chambers/Associations spread all over the country.

Vision

Empower Indian enterprise by inculcating knowledge that will be the catalyst of growth in the barrierless technology driven global market and help them upscale, align and emerge as formidable player in respective business segments.

Mission

As a representative organ of Corporate India, ASSOCHAM articulates the genuine, legitimate needs and interests of its members. Its mission is to impact the policy and legislative environment so as to foster balanced economic, industrial and social development. We believe education, IT, BT, Health, Corporate Social responsibility and environment to be the critical success factors.

Members – our strength

ASSOCHAM represents the interests of more than 4,50,000 direct and indirect members across the country. Through its heterogeneous membership, ASSOCHAM combines the entrepreneurial spirit and business acumen of owners with management skills and expertise of professionals to set itself apart as a Chamber with a difference.

Currently, ASSOCHAM has more than 100 National Councils covering the entire gamut of economic activities in India. It has been especially acknowledged as a significant voice of Indian industry in the field of Corporate Social Responsibility, Environment & Safety, HR & Labour Affairs, Corporate Governance, Information Technology, Biotechnology, Telecom, Banking & Finance, Company Law, Corporate Finance, Economic and International Affairs, Mergers & Acquisitions, Tourism, Civil Aviation, Infrastructure, Energy & Power, Education, Legal Reforms, Real Estate and Rural Development, Competency Building & Skill Development to mention a few.

Insight into 'new business models'

ASSOCHAM has been a significant contributory factor in the emergence of new-age Indian Corporates, characterized by a new mindset and global ambition for dominating the international business. The Chamber has addressed itself to the key areas like India as Investment Destination, Achieving International Competitiveness, Promoting International Trade, Corporate Strategies for Enhancing Stakeholders Value, Government Policies in sustaining India's Development, Infrastructure Development for enhancing India's Competitiveness, Building Indian MNCs, Role of Financial Sector the Catalyst for India's Transformation.

ASSOCHAM derives its strengths from the following Promoter Chambers: Bombay Chamber of Commerce & Industry, Mumbai; Cochin Chambers of Commerce & Industry, Cochin: Indian Merchant's Chamber, Mumbai; The Madras Chamber of Commerce and Industry, Chennai; PHD Chamber of Commerce and Industry, New Delhi and has over 4 Lakh Direct / Indirect members.

Together, we can make a significant difference to the burden that our nation carries and bring in a bright, new tomorrow for our nation.

Contact

ASSOCHAM Secretary General

Shri Uday Kumar Varma
E-mail: sg@assocham.com

ASSOCHAM ICT Division

Varun Aggarwal
Director & HOD
E-mail: varun.aggarwal@assocham.com

Bindya Pandey
Executive
E-mail: bindya.pandey@assocham.com

Parag Tripathi
Asst. Director
E-mail: parag.tripathi@assocham.com

Rahul Dhakal
Executive
Email: rahul.dhakal@assocham.com

EY contacts

EY Leadership team

Gaurav Taneja
National Director
Phone: +91 124 671 4990
Email: Gaurav.Taneja@in.ey.com

Nitin Bhatt
Global Leader -Risk Transformation and
India Leader - Risk Advisory Services
Phone: +91 806 727 5127
Email: Nitin.Bhatt@in.ey.com

Rahul Rishi
Partner & Leader
Advisory Services (Digital Government)
Phone: +91 116 623 3183
Email: Rahul.Rishi@in.ey.com

Burgess Cooper
Partner – Advisory Services (Cyber Security)
Phone: +91 226 192 0000
Email: Burgess.Cooper@in.ey.com

Vidur Gupta
Partner – Advisory Services (Cyber Security)
Phone: +91 124 6711380
Email: Vidur.Gupta@in.ey.com

Credits

Navin Kaul
Sr. Manager – Advisory Services
Phone: +91 116 623 1652
Email: Navin.Kaul@in.ey.com

Satyawan Yadav
Director - Advisory Services
Phone: +91 124 464 4000
Email: Satyawan.Yadav@in.ey.com

Aseem Mukhi
Sr. Manager – Advisory Services
Phone: +91 124 671 4000
Email: aseem.mukhi@in.ey.com

Sunil K Agarwal
Project Manager – Advisory Services

Ipsa Sinha
Consultant - Advisory Services

Sharmistha Mukhopadhyay
Consultant- Advisory Services

Ajitesh Rai
Consultant- Advisory Services

Hitesh Bhatia
Analyst – Advisory Services

EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
+ 91 80 2224 0696
Fax: + 91 80 2210 6000

Ground Floor, 'A' wing
Divyasree Chambers
11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: +91 80 6727 5000
Fax: +91 80 2222 9914

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: +91 172 331 7800
Fax: +91 172 331 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 6671 8000
Fax + 91 11 6671 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Noida - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500 081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur - 831 001
Tel: +91 657 663 1000
BSNL: +91 657 223 0441

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 6615 3750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E),
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000
Fax: + 91 20 6601 5900

Notes

Notes

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1808-018
ED None

RG

ASSOCHAM

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber, initiated its endeavour of value creation for Indian industries in 1920. Having in its fold more than 400 chambers and trade associations, and serving more than 4.5 lakh members from all over India, it has contributed significantly to the economy by playing a catalytic role in shaping up the trade, commerce and industrial environment of the country. It has significantly contributed in the emergence of new-age Indian corporates, characterised by a new mindset and global ambition for dominating the international business.

Known as the fountain-head of knowledge for the Indian industries, ASSOCHAM has emerged as forceful, proactive, forward looking institution that is equipped to meet the aspirations of corporate India in the new world of business.

Ready to redefine the dynamics of growth and development in the technology driven cyber age, it aims empower Indian enterprises by inculcating knowledge that will prove to be the catalyst of growth in the technology driven global market. ASSOCHAM aims to help and guide businesses to upscale, align and emerge as formidable players in their respective business segments. Its mission is to impact the policy and legislative environment so as to foster balanced economic, industrial and social development.

ASSOCHAM is working towards creating a model business environment in India that is at par with the rest of the world and that of a developed economy. It derives its strength from its promoter chambers and other industry/regional chambers/ associations spread all over the country.

ASSOCHAM corporate offices

The Associated Chambers of Commerce and Industry of India
(ASSOCHAM) 5 Sardar Patel Marg, Chankyapuri,
New Delhi – 110021
Tel: 46550555 (Hunting Line)
Fax: 011-23017008/9
Website: www.assocham.org

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers