LDRA
Software Technology

Technical White Paper

# Emerging technology trends: Skill Challenges & Opportunities for Industry & Academia

www.ldra.com

*Abstract—This whitepaper focuses on challenges related to skills & opportunities associated with emerging technology trends typified by autonomous things, IoT, and AI. We have addressed future job opportunities and the sectors that will always be in demand. Based on our internal research, we have highlighted the current and upcoming challenges for industry and academia, and proposed a model for each of them to meet these challenges. To put the challenges into context, we have also explained how best practices for embedded software safety & security can be furthered by both academia and industry to better serve the needs of critical sectors including Automotive, Aerospace, Medical Devices and Industry. The whitepaper content is designed to be useful for both industry and academia, and for anyone looking to build a future career in these areas.*

*Keywords—IoT (Internet of Things), AI (Artificial Intelligence), ML (Machine Learning), CERT, safety, security, cybersecurity, Embedded System*

## I. Introduction

The emerging trends of technology (connected, autonomous and AI/ML aided) are promising productive, comfortable and prosperous lifestyles for the masses. However, the rate of adoption of these technologies is not so promising due to a lack of competence in the development, validation and maintenance of complex intelligent systems. Furthermore, the threats generated from the potential for connected systems to be exploited are real and call for attention and planning. The major proponents of technology adoption, industry and academia, have a huge responsibility to facilitate a feasible ecosystem.

In terms of the SWOT paradigm, the promise of emerging technologies could be considered as **opportunities**, the realizable fear of vulnerable systems is one of the **threats**, the lack of preparedness from the part of academia and industry would constitute as inherent **weakness**, and an early implementation of a competency framework to embrace future technology would be labelled as a **strength**.

In this paper, we will consider various perspectives on these technological trends to reflect on how opportunities and strengths can be utilized, and how threats and weakness could be managed.

## II. Emerging Technology Trends

The top strategic technology trends for 2019 as listed by Gartner Inc. include Autonomous Things, AI-driven development, Empowered Edge, Immersive Experience (Virtual Reality, Augmented Reality, Mix Reality across multi-model devices), and Blockchain among many others [1]. The business opportunities created by any organization embracing these technologies will mean they are well placed for the future, whilst their pursuit will create new career opportunities for individuals. AI drives almost everything in the development of these systems of the future. Such systems are about merging the real world and digital world together to a new digital reality where people, process, and technologically enabled "things" can talk to each other to create a better digital experience. Any such advancement carries a burden of risks along with the opportunities. Risks include social engineering scams which could trigger ransomware by approaches like Phishing, Baiting, etc.; cyber-attacks and data breaches; lack of clear accountability in AI based decision making processes; large skills gap in emerging technologies, talent shortage and many more [2]. But managing such risks is key to unlocking opportunities.

Traditionally, embedded applications have tended to be static, fixed function, device specific implementations with a code base measured in Bytes or Kilobytes. The application of emerging technologies including AI and IoT has seen embedded systems developed with Mega and Gigabytes of code. Perhaps counter-intuitively given the declining physical size of hardware, systems are becoming ever more powerful to accommodate this rapidly increasing software footprint. For example, the Ford GT car exemplifies "Autonomous Things" with its 10 million lines of code, many more than an aircraft needs to fly (2 million lines of code for the Lockheed F-22 Raptor and 7 million lines for the 787 Dreamliner) [5]. There is a nice infographic which highlights that an average modern high-end car has approximately 100 million lines of code [6].

With this insatiable rising demand for software comes a similarly growing concern for security. Find any organization active in these new technologies, and there will be a chief information security officer (CISO) in the building with major concerns over embedded software security. Instances of ransomware are already growing at an incredibly rapid rate. As we transition to the daily use of more connected devices such as smart cars and smart watches, we anticipate that these platforms will be targeted. It is important to understand this now so that we can get ahead of it to protect businesses and consumers.

Because the application of these upwardly trending technologies is becoming part of our daily lives, we believe that safety & security should be supplemental to the basic physiological needs of food, rest and shelter.

## III. Risks Involved in Emerging Technologies

In highlighting the significant risks associated with these emerging technologies, we advocate that the management of those risks is a key to unlocking opportunities.

1. **Security**: As the world becomes increasingly interconnected through technology, security vulnerabilities emerge from its growing complexity. Unexpected interactions between hardware and software subcomponents can

magnify the impact of a vulnerability [7]. As technology continues its shift away from the PC-centric environment of the past to a cloud-based, perpetually connected world, it exposes sensitive systems and networks in ways that we never imagined.

2. **Large Skill Gap & Talent Shortage**: According to the Global Information Security Workforce Study, the cybersecurity workforce gap is on pace to hit 1.8 million by 2022. It is not just one risk alone; this talent gap exacerbates other emerging risks. In our current environment of historically low unemployment, organizations may be unable to find the talent they need to achieve their strategic objectives. With fewer workers comes more strain on those who are available. More cyberthreats can slip through the cracks when a tech employee is stretched thin, and we will see mistakes being made if there aren't well-trained employees monitoring devices, robots, AI and other tech products. Weak tech support can also hinder a technology consultancy's reputation.
3. **Accountability in AI based decision making process**: An increase in the use of AI in organizations, whether as part of decision making or key business processes, leads to a lack of clear accountability.
4. **Lack of regulatory framework**: Several start-ups are working with the emerging technologies, but they are feeling hampered by the lack of legal and regulatory framework that can help, support and encourage new ventures. Companies often look for support that can spur innovation including public/private partnerships.

   Neither technologies nor regulations are born in a vacuum. For example, when the car was originally created, we did not have a system of signs, traffic lights, traffic police, nor driver's education and regulations have developed over a period. With the rise of applications related to Autonomous Vehicles, they will also have to properly recognize the roads and signs which requires standardization of traffic regulations at least at the national level and preferably the global one. If countries have different signage, autonomous vehicles will have to be programmed to know which countries they are in and thus how to read the signs. Standardization and regulation can make this process more straightforward and safer.
5. **Lack of collaboration with standard bodies & certification agencies**: We believe that the future belongs to those who collaborate. If everyone is moving forward together, then success takes care of itself, but any lack of collaboration presents a great risk to the adoption of these emerging technologies. There is an urgent need that the standard bodies and certification agencies should come together and collaborate to address the challenges.
6. **Cost of education and certification in cybersecurity**: One of the most important challenges in front of young engineers is that they are unclear about the career opportunities in cybersecurity related roles. Even for those who are convinced about the potential for such a career, the cost of education and certification in cybersecurity is very high and so relatively few young people are motivated to pursue related courses. As an example, the fee for the "CERT Secure Coding in C and C++ Professional Certificate" eLearning course is 1250 US$ which is approx. 89 thousand Indian Rupee [9].

   However, initiatives like Cyber Shikshaa [4] from the Data Security Council of India & Microsoft in India are welcome steps. This particular initiative aims to upgrade skills for women in the niche area of cybersecurity and hence to increase women's participation in cybersecurity roles. Worldwide, in 2018 women made up 24% of the skilled cybersecurity workforce [3].

## IV. Impact of Automation

A report titled "Artificial Intelligence, Automation, and the Economy" released by the Executive Office of the President of the United States in December 2016 highlights that the increasing uptake of automation through AI capabilities will disrupt the livelihoods of millions of Americans. The report mentions that AI will change the type of jobs available, the skills workers need to thrive, and the importance of education & training for the jobs of the future.

Our market research team has investigated this further and found that automation in coming years will have a significant impact on the economy. Many low skilled jobs will be lost but at the same time, many high skills jobs will be created. The potential for automation to cause mass unemployment places the responsibility for readying young engineers squarely on the universities. Only then will industry have access to the suitably skilled workforce needed for a safe & secure tomorrow.

*A. Low–Skilled and Highly–Skilled Jobs*

Suppose we can categorize highly skilled jobs as those requiring formal educational qualifications, creative problem-solving skills, business analytics, creative thinking, and strong communication skills, and less skilled jobs as those which instead require specialization in a task which follows a set of processes and is repetitive in nature. We advocate that the usefulness of the skill set possessed by an individual on this scale (low to high) will not be directly proportional to a particular degree classification or level of education because there is no uniform education system worldwide. There are huge gaps in the syllabi of many universities, and many do not meet industry's expectations.

During an economic downturn or recession, low skilled workers may be displaced from their jobs by better qualified workers and it is therefore important that we develop a habit of learn, unlearn and relearn. To stay employed and move up the value chain, people with mid-level job skills need to pick up new skills to match the latest business innovations.
The emerging technologies highlighted by the Gartner study including the Internet of Things, Deep Learning, Artificial Intelligence, Data Scientists, Cyber/Information Security, and Cognitive Computing, have caused a change in the entire ecosystem, creating a new set of jobs which requires a new and different set of skills. The World Economic Forum's "Top 10 emerging technologies that will change our lives" extends that list to include nanosensors and the Internet of Nano-Things, next-generation batteries, blockchain, autonomous vehicles, organs on chips, and the open A.I. ecosystem.

## V. Needs of Industry & Academia

*Industry*:
In this context, we have found that there is a significant disconnect between industry & academia. Industry always finds it tough to get the right set of people on board, and yet there are countless engineering graduates who believe that they have appropriate skills but are unable to find a job. When we analysed this sad fact, we found that that the primary problem is that students are focused on the completion of their four year degree programme, rather than on the skills required by industry. By refocusing on the acquisition of the skills most in demand, the challenges faced by both the individual and by industry can be met.

In today's world where start-ups proliferate, competition is fierce and technology is soon outdated, small employers cannot afford to employ fresh engineering graduates and to invest 3-4 months on training them. Instead, they expect that at least some basic knowledge of the skills needed by industry should be acquired during academic studies so that with a little polishing, they can be deployed on real projects. The minimum expectation of companies is that potential employees should be able to write a decent piece of code to address a given problem, and to then debug it such that the result is a working program. According to industry reports, only 4.51% of candidates possess such skills and are software industry ready.

To cite another example, many candidates are aware that they should avoid problems like buffer overflow and null pointer dereferencing. That is a good thing, but our research suggests that much fewer candidates really know the key reasons why we should avoid these issues, and what happens if we don't. This ability to reason and address complex problems such as these should be developed at the academic level to prepare candidates for industry.

*Academia*:
It would be easy to reduce the problem to a "blame game", because a common stance in both industry and academia is to suggest that each isn't supported by the other. In fact, a report on the problem by the Government of India's Ministry of Skill Development and Entrepreneurship highlighted the lack of integrated onsite apprenticeship training, insufficient funding and shortage of qualified trainers among others [10]. Academia needs strong support from industry in any of various forms including the delivery of guest lectures, experiential on-the-job training/internship for students, and support in upgrading skills within faculties through faculty development programmes and/or industry driven webinars. Exposure of students and research scholars to live projects based on developing technologies like AI and Autonomous Things would benefit industry and academia alike.

## VI. Challenges with the Current Academia Model

A recent report entitled "National Employability Report" by the Aspiring Minds organization highlights the fact that 90.72% of graduating engineers do not have the programming and algorithm skills required by IT product companies. For example, companies will always prefer a candidate who can; write clean, readable, testable and maintainable code, have the ability to debug programs, and can demonstrate complex problem solving and analytical skills, over a candidate who can only write a program which is functionally correct.

In our view, this highlights several major challenges.

1. **Syllabus**: In many universities, students are being trained for jobs that no longer exist. Higher education needs to accept that it has to offer job-friendly syllabi. The prime responsibility for the development of young professionals with employable skills in emerging technologies rests with our institutes of higher learning. Unfortunately, our present higher education system as reflected in many universities is completely incapable of fulfilling this responsibility even at the most basic level.
2. **Teaching**: A good teacher would never issue a set of instructions without explanation. Instead, they would give their students the knowledge to equip them to decide what would be the best course of action to take in a given situation. A good teacher can inspire hope, ignite the imagination, and instil a love of learning. But unfortunately, there is a long held belief that teaching is a fall-back position for anyone who can't find a job. That is a problem, and it is exacerbated by faculties that lack in industry exposure and rigidly

follow traditional teaching methodologies. The root causes of this intransigence may include disinterested management, a resistance to learning new things by faculty staff, or an underlying concern amongst management that empowered faculty members may become equipped to leave their institute.

3. **Framework**: Emerging technologies require an interdisciplinary approach. For example, a project related to autonomous driving may require active participation from various departments such as Design, Mechanical, Electrical, Electronics, Computer Science, and Software Systems. There is often no such approach in academia
4. **Learning**: We have seen several engineering students taking training capsules to supplement their engineering training, when the supplementary capsule content should have been a core part of their primary qualification. In particular, academia needs to focus on building skills in innovation, creativity, and problem-solving.

## VII. Proposed Model for Academia

*Curriculum*
Academia needs to adopt technological curricula that cater for the broader needs of campaigns like "Make in India", "Digital India", etc, and review them every year. It should integrate vocational courses in curricula and have them reviewed by industry leaders. For example, specific topics such as software engineering, software testing, secure coding, and verification & validation of systems, are still treated as elective subjects in many universities across the globe. It is high time for leading universities to come forward and mandate those subjects to provide a sound and current software engineering foundation that caters for the needs of all emerging technology trends. Early this year, LinkedIn identified 25 Hard Skills and 5 Soft Skills [11] they believe will be in big demand in 2019. It is no surprise that the list includes software testing because the number of new software applications hitting the market is at an all-time high – and that implies a need for more and more people who can ensure they all work.

*Faculty Development*
College management should focus on training the trainers in emerging technologies. Academia should plan industrial visits for students and research scholars so that they can learn about the technologies involved and get exposure to real-life projects.

*Teaching Methodologies*
Academia should accommodate industry led projects in the final semester and adopt comprehensive skill-based learning paths. Job orientated training capsules should be planned during the engineering courses themselves with the focus of creating employable, skilled engineers. Academia should also encourage students to acquire additional skills by leveraging new training methods like MOOC (Massive Open Online Course) platforms and other digital learning models.

*Projects*
Academia should encourage interdisciplinary projects that look to solve the problems of society & industries. The aim should be for every project to transition into products. Colleges should have entrepreneurship clubs or incubation centres to help entrepreneurial students with funding, tools, technologies, business skills, and legal advice.

*Regulation*
There is a need to have appropriate regulatory framework that encourages world class excellence. At the same time, we need to relook at the ranking parameters. Government should also allow foreign universities to open centres in India with an objective to boost competition among universities.

*Vocational focus*
Universities should intensify the vocational focus of their degrees beyond that of courses such as Computer Science, Electronics & Communications, and Mechanical Science. Graduates of more focused courses would be equipped with skills for a specific sector, as compared with a generic degree which merely equips graduates to be a "Jack of all trades, master of none". For example, IIT Hyderabad (India), Carnegie Mellon University, and Massachusetts Institute of Technology (MIT) (U.S.) offer B. Tech. courses in Artificial Intelligence. The course at IIT Hyderabad focuses on industry verticals such as healthcare, agriculture, smart mobility, and many others. Although we advocate skills-based degrees, these courses must mitigate the risks inherent in such an approach to fast-changing technologies. Including core fundamentals would provide some protection to students should the primary focus of a course become a defunct technology, which could otherwise result in a further widening of the gap between industry & academia.

## VIII. Proposed Model for Industry

Industry also has a part to play in bridging the gap to academia. Technologically led industries should take the initiative and put immediate commercial gain aside to train faculty members on the latest technologies. Teachers create the destiny of a nation so if we fail to support them, then we are also failing the country. Additionally, industry should also help academia to frame syllabi and ensure that academia is equipped with the right set of technology, course materials, tools, etc. to teach students on next generation skills.

Industries have a vital role to play in improving the academic ecosystem. Employees should be motivated to contribute to the society that helped educate them. We feel that industry should help academia by offering on-the-job training, providing internship opportunities, delivering

guest lectures, and conducting webinars on emerging technologies. It would also be mutually beneficial for industry to involve academia in their R&D activities so that academic researchers and undergraduates can contribute to cutting edge technology, whilst gaining real world experiences.

We have seen tech companies struggle to find fresh engineering graduates with the right set of skills, and eventually recruit experienced candidates instead which adds to the overall cost. But industry should acknowledge the fact that if we don't plant seeds today, there will be no fruit tomorrow. In short, they need to invest in the education system if they want to have appropriately skilled, new engineering graduates in the future. Such investment would be to the benefit of the investor, the academic community, and the nation.

With the help of a government stakeholder, industry should also take initiatives at national level to spread awareness of emerging technology trends. For example, Finland has launched an ambitious challenge to teach the basics of A.I. to 1% of its population, or about 55,000 people, to establish the country as a leader in applying and using that advanced technology [12].

## IX. Best Practices for Embedded Software Safety & Security

One of LinkedIn's "Skills in big demand" for 2019 was software test. As an example of how the academia and industry might fuse better in handling cutting-edge technology, consider the best practices for embedded software safety and security in that context, and how they might become features of focused vocational courses, equipping students with skills that industry can apply.

1. **Identification of safety & security integrity level of a system**: The level of effort to be expended in verification and validation of a safety-critical application should be proportionate to the consequence of its failure. For example, the validation and verification overhead for an entertainment system will be proportionately less than that for a flight control system. The enumeration of that effort involves an assessment of the system's severity, exposure and controllability which are then used to identify an appropriate safety integrity level (SIL). NIST Cybersecurity and other frameworks use similar a notion to determine security levels. The principles of such assessments have been consistent for many years. However, the functional safety cybersecurity standards to which they usually relate are regularly updated, and that would need to be reflected in the syllabi.
2. **Make compliance with secure coding standards a part of university culture**: We have observed that at this time, coding standards are not featured as part of curricula. Academia should include the study of coding standards like CERT C/C++ and MISRA C/C++ as a part of their courses and keep copies of these standards in their digital libraries so that students can access them. Learning good habits are always important, hence at the very first instance when a student learns C/C++ language, they should be learn to program in accordance with coding standards. Such a move would have a long term positive impact in the society, and students will be ready to fulfil industry's needs.
3. **Follow Industry best practices such as "Top 10 Secure Coding Best Practices" by SEI CERT**: In a world prone to cyberattack and where new types of threats such as side channel attacks and zero-day vulnerabilities emerge on an ongoing basis, no one tool or other defence can assure 100% software safety & security. Hence it is recommended that researchers & industry experts should regularly exchange thoughts and ideas with reference to current best practices such as the Top 10 Secure Coding Best Practices published by SEI CERT. Course content should be dynamic and flexible in nature, allowing students to study state-of-the-art subject matter.
4. **Write good quality code**: Anyone may claim that they have written high quality code, but students need to learn of the benefit of metrics to enumerate quality. Quality standards such as those provided by CISQ (Consortium for IT Software Quality) define each quality characteristic at the code unit level and system level. There are numerous metrics to consider including the number of comments, number of comments in headers, depth of loop nesting, cyclomatic complexity, fan in/out, number of operands, unreachable lines & branches, number of procedures, and number of knots. It is important to prepare a list of the quality metrics to be applied to a particular project, and to adhere to it. Learning how to do so will require automated tools to be accessible to students.
5. **Code Coverage should be 100%**: No critical code should include dead code or unreachable code. Students should learn the benefits of code coverage analysis, and the different measures and techniques available depending on the criticality of the system under review, such as statement coverage, branch coverage, MC/DC, LCSAJ, data flow analysis, and control flow analysis.
6. **Establish a requirements traceability matrix**: Courses should teach the fundamental principle of bidirectional requirements traceability, as promoted by most cybersecurity and functional safety standards. The objectives are to confirm not only that all functional, functional safety, and cybersecurity requirements have been implemented, but also there is no surplus code that fulfils no project requirement. Teachings should also reflect the fact that live projects are usually subjected to changing

requirements, and that bidirectional traceability across the entire V model (High Level Requirement to Low Level Requirement to Source Code to Test Plan) is also beneficial for impact analysis and for optimization of the attack surface.

7. **Apply both proactive and reactive test methods**: Traditional enterprise level cybersecurity test techniques do have a place, but they tend to be reactive in nature. Courses should reflect the fact that although testing to prove the resilience of application code is important, it cannot be as effective in isolation as an approach that also embraces designed-in security, verified by proactive testing during development.
8. **Target based testing is important**: Although any testing is potentially beneficial, the closer the test environment is to the environment intended for the live application, the better. This is desirable for all software, and its importance is proportional to the criticality of the software as reflected by its Safety Integrity Level (point 1 above).
9. **Standards based approach**: We should promote the notion that standards don't prevent innovation or industry growth, but rather that they boost confidence in the technology and help in the creation of better, more reliable products. Courses should include reference to prominent standards, and industry should look to follow functional safety, cybersecurity and process standards. A table describing prominent functional safety & cyber security standards is shown below.

| Industry | Functional Safety/ Process Standard | Cyber Security Standard |
|---|---|---|
| Automotive | ISO 26262 | SAE J3061 |
| Railways | EN 50128 | ISA/IEC 62443 |
| Industrial | IEC 61508 | ISA/IEC 62443 |
| Nuclear | IEC 60880 | ISA/IEC 62443 |
| Medical Devices | IEC 62304 | ISA/IEC 62443 |
| Avionics | DO–178B/C | DO–326A |

10. **Use Qualified Tools**: Many of these standards insist that tools should be proven to an appropriate level of confidence for the environment in which they are to be applied, and that a formal "tool qualification" process is followed. DO-330, for example, provides tool-specific guidance for building airborne and ground-based software. However, the same principle holds true irrespective of the field in which it is applied. If a test tool isn't trustworthy, what is the point of using it?

## X. How real are these security threats?

Building further on Embedded Software Safety & Security as an example of how technologies might be better adopted across industry and academia, it is important to understand that these practices are designed to address very real threats and dangers. For example:

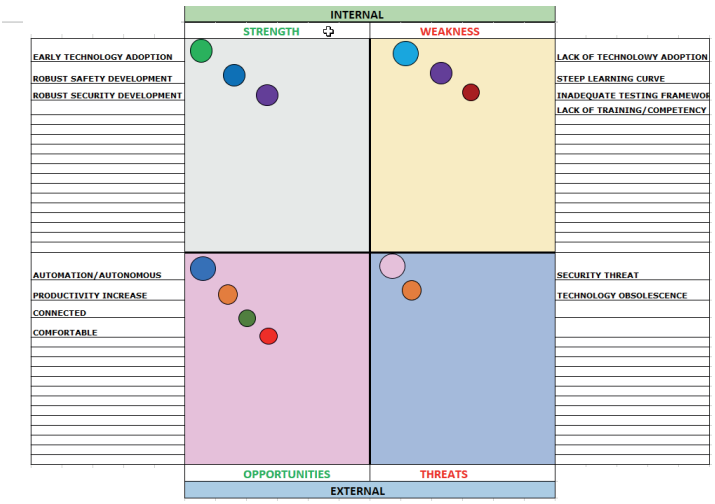
Example 1: Ethereum is second largest digital currency in the world (after Bitcoin). Recently, a group of hackers stole $31M worth of Ether in few minutes; a situation that could have been much worse had white hat hackers not intervened. This event has sent out a message to the world of Blockchain technology that security must be a top priority.

Example 2: In 2015, security researchers Charlie Miller and Chris Valasek hacked a Jeep Cherokee [8] to prove that the Jeep could be remotely accessed while driving down the road via vehicle's internal network – in this case, a CAN bus. This attack, amongst others, has ensured that developers of autonomous vehicles are now embracing cybersecurity as a necessary component of their technology stacks.

Example 3: In March 2018 one of Uber's self-driving vehicles killed a pedestrian in a Phoenix suburb, resulting in the suspension of the company's right to operate autonomous cars on public roads in Arizona. Such an event emphasizes the need for proper validation.

## XI. Summary & Recommendation

Referring back to the SWOT paradigm discussed at the outset, it is useful to represent the characteristics of the emerging technologies in a SWOT diagram.



Some of these emerging technologies could affect the lives of billions, including the top 10 trends suggested by Gartner:

1. Autonomous Things
2. Augmented Analytics
3. AI Driven Development
4. Digital Twins
5. Empowered Edge
6. Immersive Experience
7. Blockchain
8. Smart Spaces
9. Digital Ethics & Privacy
10. Quantum Computing

If the opportunities of these and other emerging technologies are to be grasped and the threats they pose adequately dealt with, it is imperative that industry and academia become mutually supportive. The adoption of best practices in embedded software safety and security across industry and academia, provides a good example of how improved co-operation can help.

## XII. Conclusion

We have explored various facets of technology adoption from the perspective of multiple stakeholders. To garner sustainable, usable benefits from technology, stakeholders should work in a synergetic way, and in particular academia and industry need to co-operate more effectively if the potential of emerging technologies is to be optimized.

Although this is true of most areas of cutting-edge technology, it is especially pertinent of testing for safety and security in embedded software applications (itself a part of LinkedIn's "Skills in big demand" for 2019). Amidst all the rush to push other technological boundaries, it is one trend we can not afford to compromise.

## References


[1] https://www.youtube.com/watch?v=nRTRyfIDp4k
[2] Gartner Top 10 Emerging Risks of 3Q18 (Gartner Risk Management Leadership Council)
[3] ISC2 Cyber Security Workforce Study 2018
[4] https://www.dsci.in/cyber-shikshaa/ Project Cyber Shikshaa by Data Security Council of India
[5] https://www.motorauthority.com/news/1098308_the-ford-gt-has-more-lines-of-code-than-a- boeing-passenger-jet
[6] https://informationisbeautiful.net/visualizations/million-lines-of-code/
[7] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf
[8] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[9] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V35
[10] Report of the Committee for Rationalization & Optimization of the Functioning of the sector skills council by Ministry of Skill Development and Entrepreneurship, Govt. of India http://msde.gov.in/assets/images/ssc-reports/SSC%20Vol%201.pdf
[11] The Skills companies need most in 2019 – And how to learn them. https://www.linkedin.com/pulse/skills-companies-need-most-2019-how-learn-them-paul-petrone/
[12] https://www.technologyreview.com/the-download/612762/a-countrys-ambitious-plan-to-teach-anyone-the-basics-of-ai/


## Authors


*Shinto Joseph, Director*
*South East Asia Operations at LDRA India*

*Himalya Bansal, Account Manager*
*LDRA Academic Alliance Program at LDRA India*