Editors are used in diverse industries and for many types of products, such as magazines, newspapers, blogs, and books. There are certain beauties an editor must possess. S/he is a one who could be inquisitive, imaginative and detail leaning. S/he should have needed first-rate listening and verbal communication skills and should be contented using computers to do their work and need good interpersonal and writing skills. In Cybernomics modus-operandi of editing is bifurcated in three levels. They are recognized as substantive, copyediting and proofreading. Finally the editor assesses the rationale of the text, who will read it and why. An editor is a decisive booklover and a devotee of words, whose position is to buff up and purify an article. Editors are accountable for checking facts, spelling, grammar, and punctuation. They are also accountable for ensuring that an article corresponds with in-house style guides and feels polished and refined when done. There are also times when editors need to step in and cut out what doesn't fit the purpose of the story and guide the attention towards the areas that the reading audience should focus on. The existing editorial team that is entirely engaged and fanatical to the accomplishment of these outstanding periodicals. In this new era of Cyber there are a numeral changes that we would like to exemplify attention to the periodical's readers, as we are self- assured such changes will plead to a widespread range of academic and information technology interests. Cybernomics is a cooperatively designed by our leadership team that aims to symbolize the comprehensive network of our community from cyber society to the cyber users.

The impression of a magazine (Cybernomics) was developing for in excess of a few years and finally we are one month away from 2020 which is on the verge of completion. Being an editor I am extremely obliged and privileged to Scholastic seed Inc. which is an upcoming "*Publishing Aggregator & Periodical Mentor"* and indebted for providing me an opportunity during its 2nd Annual General meeting vide resolution no. RN/SSI/CYBNM/1APR2019 dated 1st April, 2019. We are also much engorged with self-satisfaction to be working in tandem with an outstanding team of entire editorial team and its New Delhi office. We make out the implication of ensuring that our initiatives in an academic format would represent the work and research being conducted in all regions of the planet, and at the same time also highlights key issues significant to technocrats not only in urbanized countries but also in low-resource countries. Second, the periodical will attribute various kinds of articles that glass case imperative issues related to cyber and burgeoning terms which revolves around it. The reply to our plea to authors for contribution has been devastating. In spite of our superlative hard work, due to an assessment of editorial board and the referee review board, some of the articles/papers could not be incorporated in the present issue of Dec 2019, but this shall not put a ceiling on any of the authors to send their original articles in the form of a Experimental Research Paper (ERP), Argument Based Credential (ABC), Theme based paper (TBP), Scrutiny Tip (ST), Case Study (CS) , Column (CLM), research reviews or empirical contributions for publication in our magazine Cybernomics. As an editor, and on behalf of our editorial team we are au fait with the value authors place on high-quality and unbiased peer review conducted in a suitable form. In accumulation, we value the consequence of rapid publication, and so to that end we have structured our editorial team to encompass Associate Editors, a Social Media Editor, and a Video Editor so we are capable to expedite the processing of submitted manuscripts. We have instructed all those involved with the periodical in an endeavor to endow with the highest standard of script review, editing, and publishing. We have implemented meticulous peer review decisive factor, and this will be replicated in the quality of published articles. We also want to plead with all those who are mesmerized in being part of this energetic and obsessive team to get in contact with us, as we will greet your attachment. We persuade colleagues working in related disciplines of cyber and Information technology as an appropriate medium for the publication of your own high-quality research.

Thank you and acknowledgement

I am opportune to have worked with such a enormous squad of contributors. It was an honor to incarcerate their thoughts and systematize them for the readers. I would like to thank all the contributing authors for their submissions. They are the true rock stars who have given us their know-how first handily, their name and their trust on this particular write-ups. They ought to have credit for the success of the magazine Cybernomics.

Subodh Kesharwani
Editor

The rationale behind writing a note on behalf of an editor bench on this meticulous subject matter "Responsibility of Artificial Intelligence in creating Cyber Security among the peers" is well designed and premeditated for this fastidious issue (volume-1 No.--7 December 2019) due to advent of technology in all the phase. In entirety we had acknowledged twelve articles in various capacities with blended approach and manifestation. The earliest and major articles categorization is Experimental Research Paper (ERP) and talks about "Security issues with the four-layer architecture of IoT model". Next three articles nomenclature is Argument Based Credential (ABC) and is entitled as "Augmented Reality: The present and the Future", "Big Tech Monopoly - Effects, Desirability and Viable Regulations" and "Digital Forensics: 2020 (Seeds are Sown)". The third Category is Theme based Paper (TBP) entitled "Curtain Raiser to Big Data". The fourth segregation is Scrutiny Tip (ST) consist of three articles in which we had three articles entitled "Manipulators on Internet in A Cyber Era", "3D Internet (The Virtual World)" and "Lighting up the Dark Web" The fifth category is Case Study (CS) entitled "Artificial Intelligence in Gaming" and sixth category is Column (CLM) which revolves around two articles "How Will Block chain Revolutionize Biotechnology? And "Do you think Cyber security is a new concept? Think again".

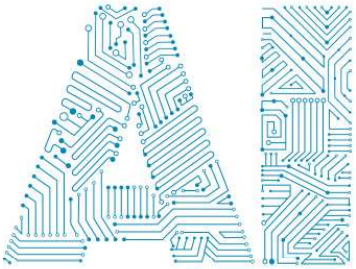
And finally the last section is View point (VP) consisting of an article on "Industry 4.0: Some Facts & and figures". We had also created some more innovative thoughts in this particular issue which is an innovation and creation of editorial office such as Book Review, Award, and Biographical note of a luminary in an area of cyber. We had also used some filler which can definitely work as teasers such as cyber thought, Cyber Journal, Cyber Books, Do You know and other trends and changes occurred in the cyber world. These heads are supposed to be placed in between or at the end of articles for the reader with an intention to make the reader an agile and aware about the contemporary trends going on in the cyber world. There are certain prefixes which would be common in all the heads.

Behind every enormous writer, there's a great editor team. But what exactly do they perform? How do they toil? What goes through their mind when a brief gets mangled or copy comes behind schedule? This is all about editorial team who rigorously works day and night to streamline the publishing schedule and accomplish the timely delivery. Manuscript submissions are being accepted for Volume-2, Issue-1, January, 2020 which will be in the new avatar and would be formulated with a fresh principle of authors. The original articles can be submitted to the Editor (Word document, by email only, at scholastic.seed@gmail.com or at editorial.scholastic.seed@gmail.com or http://www.cybernomics.in/index.php/cnm/about/submissions. Articles for columns should be prearranged with the particular column editor/s. It is requested by authors to go through the portal and make out the trend of articles the magazine published at www.cybernomics.in. Cybernomics is a true podium for academicians, industry executives, researchers and students for sharing the views and the news of the management in terms of research papers, articles and case analysis, reviews etc. the more detail of the nomenclature is mentioned in a booklet and obtainable online at www.cybernomics.in . We are stiff about the ensuing issues of the magazine with regard to distinction and disclosure. We hope that within a short period this monthly bulletin will make the academicians, industry executives, researchers and students to travel from the point of recognizing something to part with the whole thing. We wish the periodicals for its effort and intransigence of its rhythm in the same direction in the days to come. Our genuine thanks to all the contributors for their shore up and consideration and publisher Scholastic Seed Inc... We are yet again concerned for all academicians and researchers to boost their unpublished articles/papers for publication in our periodical to figure out the economics of Cyber.

Responsibility of Artificial Intelligence in creating Cyber Security among the Peers

The earth is going digital at an unprecedentedly quick rapidity, and the transformation is only going to go still faster. The digitalization means the whole thing is moving at lightning speed – business, entertainment, trends, new products, etc. The consumer gets what he or she wants instantly because the service provider has the means to deliver it. The cyber security risk countryside is persistently evolving, and regulations like GDPR are making it even more decisive for organizations to shelter their customers' and users' privacy. As cyber attacks cultivate in quantity and density, artificial intelligence (AI) is helping under-resourced security operations analysts keep on ahead of threats.

Emerging technologies put cyber security at jeopardy. Even the new advancements in self-protective strategies of security professionals do not succeed at some point. Besides, as offensive-defensive strategies and innovations are running in a never-ending cycle, the intricacy and volume of cyber attacks have amplified. Combining the potency of artificial intelligence (AI) with cyber security, security professionals have additional resources to defend vulnerable networks and data from cyber attackers.

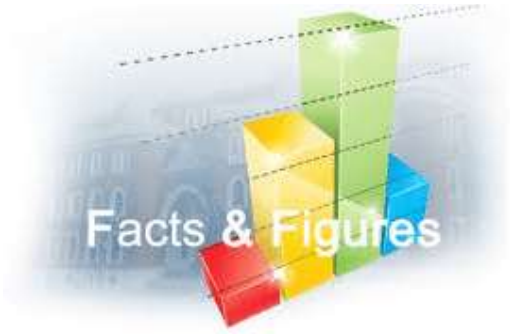


From Google and Amazon to Apple and Microsoft, every foremost technological group is dedicating resources to infiltrate in artificial intelligence. Personal assistants like Siri and Alexa have made AI a part of our everyday lives. In the meantime, revolutionary breakthroughs like self-driving cars may not be the model, but are positively within reach. Artificial intelligence (AI) is the leisure of human intelligence processes by machines, predominantly computer systems. These processes squeeze learning (the acquisition of information and rules for using the information), reasoning (using rules to reach inexact or specific conclusions) and self-correction. Artificial intelligence (AI) is one of the uninterrupted buzzwords of computer science. Many cyber security providers now proffer products that influence artificial intelligence and machine learning (ML) to facilitate exposure and rejoinder to cyber threats. On one hand, artificial intelligence in cyber security is helpful for the reason that it gets better how security specialists scrutinize, study, and be thankful for cybercrime. It enhances the cyber security technologies that companies use to clash cybercriminals and assist keep organizations and customers safe. On the other hand, artificial intelligence can be very resource exhaustive. It may not be straightforward in all applications. More significantly, it also can dole out as a new weapon in the arsenal of cybercriminals who use the know-how to grind and progress their cyber attacks.

Modus-Operandi of AI Vis-À-Vis Securing Cyber

- AI will drastically transform the kinds of work cyber engineers are doing. In order for IT teams to successfully implement AI technologies, they will need a new category of experts to train the AI technology, run it, and analyze the results
- Using AI for cyber security enables organisations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify threats and incidents, investigate them, and remediate incidents.
- Data security is now more vital than ever. Updating existing cybersecurity solutions and enforcing every possible applicable security layer doesn't ensure that your data is breach-proof.

Some Facts and Figure Related to Cyber Threats

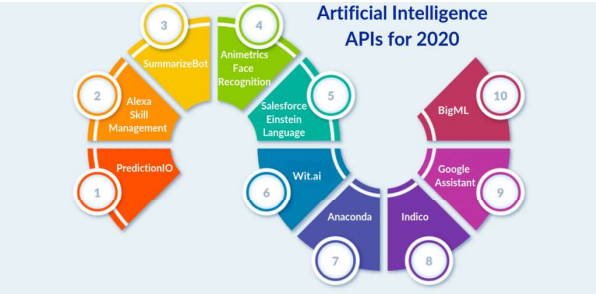


- Cybercriminals, if they get access to the security firm, can alter the label as per their convenience.
- Data capital will replace big data as the big topic of boardroom conversation.
- internal threats represent 60% of cyber security attacks
- Over 90% of data breaches and cyber attacks aren't caused by hackers an ocean away, but by an employee

who accidentally opened a spam email or sent their password over unencrypted email or submitted data to an unencrypted website.

- Phishing emails are extremely prevalent; one in every 99 emails is a phishing attack. Fortunately, AI-ML may play a significant role in preventing and deterring phishing attacks.
- The AI software architecture can also work in different lighting conditions and compensate for changes like getting a new hairstyle, growing facial hair, wearing a hat, etc.
- There have been over 2,000 unique vulnerabilities reported. Managing all of these with human resources or traditional technology is extremely difficult. AI, however, can tackle this with a lot more ease
- What is changing, and will become only more apparent in 2020, is the size of the attack surface and the velocity of the attacks themselves

AI Security used by Technological Business Tycoons



Acknowledged: Signity solutions have used an APIs which are commonly used in the artificial intelligence (AI) industry.

Source: https://www.signitysolutions.com/blog/artificial-intelligence-apis

- Eye builds the vision algorithms, software and hardware that ultimately become the eyes of autonomous vehicles.
- Alphabet is Google's parent company. Waymo, the company's self-driving technology division, began as a project at Google. Today, Waymo wants to bring self-driving technology to the world to not only to move people around, but to reduce the number of crashes.
- AlphaSense is an AI-powered search engine designed to help investment firms, banks and Fortune 500 companies find important information within transcripts, filings, news and research.
- Amazon uses artificial intelligence to ship things to you before you even think about buying it. They collect a lot of data about each person's buying habits and have such confidence in how the data they collect helps them recommend items to its customers and now predict what they need even before they need it by using predictive analytics.
- Apple's face recognition technology, used on its iPhone X devices, is one example. Called 'Face ID,' the technology works by processing the user's facial features through built-in infra-red sensors and neural engines.
- Balbix platform uses AI-powered risk predictions to protect the IT infrastructure against data and security breaches.
- Blue River Tech combines artificial intelligence and computer vision to build smarter farm tech. The company's See & Spray machine learning technology,
- Capgemini Research Institute analyzed the role of cyber security and their report "Reinventing Cyber security with Artificial Intelligence" indicates that building up cyber security defenses with AI is imperative for organizations.
- Casetext is an AI-powered legal search engine with a database of more than 10 million statutes, cases and regulations. Called CARA A.I.
- Chinese company Alibaba is the world's largest e-commerce platform that sells more than Amazon and eBay combined. Artificial intelligence (AI) is integral in Alibaba's daily operations and is used to predict what customers might want to buy.
- Clarifai is an image recognition platform that helps users organize, curate, filter and search their media. Within the platform, images and videos are tagged, teaching the intelligent technology to learn which objects are displayed in a piece of media.
- CloudMinds provides cloud robot services for the finance, healthcare, manufacturing, power utilities, public sector and enterprise mobility industries.
- DataRobot provides data scientists with a platform for building and deploying machine learning models. The software helps companies solve challenges by finding the best predictive model for their data.
- Figure Eight provides AI training software to machine learning and data science teams. The company's "human-in-the-loop" platform uses human intelligence to train and test machine learning.
- Freenome uses artificial intelligence to conduct innovative cancer screenings and diagnostic tests. Using non-invasive blood tests, the company's AI technology recognizes disease-associated patterns
- Gmail uses machine learning to block 100 million spam in a day.
- Google is using Deep Learning AI on its Cloud Video Intelligence platform
- H2O.ai is the creator of H2O, an open source platform for data science and machine learning that is utilized by thousands of organizations worldwide.
- IBM's Watson cognitive training uses machine learning to detect cyber threats and other cybersecurity solutions.
- Narrative Science creates natural language generation (NLG) technology that can translate data into stories.
- Nauto builds autonomous mobility software to create smarter commercial fleets and safer drivers. The smart technology detects distracted driving, coaches drivers on safety and alerts them to risks ahead.
- Neurala is developing "The Neurala Brain," a deep learning neural network software that makes devices like cameras, phones and drones smarter and easier to use.
- nuTonomy is developing software that powers autonomous vehicles in cities around the world. The company uses AI to combine mapping, perception, motion planning, control and decision making into software designed to eliminate driver-error accidents.

- OpenAI is a nonprofit research company with a mission to create safe artificial general intelligence (AGI). AGI aims to create machines with general purpose intelligence similar to human beings.
- Persado is a marketing language cloud that uses AI-generated language to craft advertising for targeted audiences.
- SoundHound Inc. is all about audio, providing multiple solutions that utilize voice and conversational intelligence. Tempus uses AI to gather and analyze massive pools of medical and clinical data at scale.
- Vidado can pull data from virtually any channel, including handwritten documents, dramatically increasing paper to digital workflow speeds and accuracy.
- x.ai creates autonomous personal assistants powered by intelligent technology. The assistants, simply named Amy and Andrew Ingram, integrate with programs like Outlook, Google, Office 365 and Slack, schedule or update meetings, and continually learn from every interaction.
- Zymergen is utilizing machine learning, automation and genomics to accelerate the advancement of science. Spanning the agriculture, pharmaceutical and chemical industry, the company enables faster cultivation of microbes through automation software and a huge catalog of physical and digital DNA data.

There are a few other significant benefits of an AI, which includes –

- Detects malicious activities and stops cyber attacks
- Analyzes mobile endpoints for cyber threats – Google is already using machine learning for the same
- Improves human analysis – from malicious attack detection to endpoint protection
- Uses in automating mundane security tasks
- No zero-day vulnerabilities

Innovation over and above the AI/ML/DL

- Samara is Airbnb in-house innovation design studio, working on exploring new ways to expand the company's mission, through projects related to design, architecture, hardware and software engineering.
- The Innovative Side of the Company: Lab126 represents the inventive side of Amazon. The creative hub where new consumer electronics devices are thought and developed
- AT&T Labs is the hub where scientists and engineers work to create the disruptive innovation that will lead to the future.

AI and Machine Learning (ML) have been the "silver bullets" of security conscientiousness for the past few years. Malicious actors are taking note. For case in point, just like security vendors can teach their ML models on malware samples to identify them, malware writers can "train" or refrain their malware to avoid revealing using the same exact algorithms. Attackers can also eradicate the data that ML models use in training.

Conclusion

If we do not have the aptitude strength to safeguard our data in technology such as IoT, block chain, artificial intelligence, machine learning, and other emerging technologies, we are going to see a danger of breaches and loss of data. Technology is outpacing existing regulations and observance frameworks, so we need to make sure developers and manufactures that the responsibility on themselves for the good of the consumer. Like any other cyber security solution, AI is not 100% fail-safe. It is a double-edged weapon with the capability to limit cyber-attacks and mechanize mundane routine tasks, and yet, it's a blessing. The automation gesticulate will take over day after day tasks while the same technology will augment the chances of fewer human errors and in attention.

Scholastic Seed Inc.
www.scholasticseed.in