ISACA
Bangalore Chapter

Q4 - 2023 ISSUE

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

Congratulations!
ISACA
2024
OUTSTANDING CHAPTER
ACHIEVEMENT AWARD
26th Annual Karnataka Conference
ISACA Bangalore Chapter
28th & 2
The Lalit Ashok - Bangalore
A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Thr ts
BRONZ

ISACA BANGALORE CHAPTER FOR OUTSTANDING CHAPTER ACHIEVEMENT AWARD !!!

ISACA® Executive Committee 2023 -2024

Bangalore Chapter

President

Mr. Rajasekharan K R

Vice President

Ms. S Vijayavanitha

Secretary

Mr. Deepak G B

Immediate Past President

Mr. Velmuruga Venkatesh

Treasurer

Ms. Suma K V

Director – Programs

Mr. T R Rajesh

Director – Web Services

Mr. Raghava Rachuri

Director – Membership

Mr. Narasimhan Elangovan

Director – Marketing

CA. Chandra Prakash Jain

Director – Newsletter

Mr. Pramod C B

Director – SIG

Ms. Lalitha Satheesh

Director – Research & GRA

Mr. Akhilesh B

Coordinator – CISM,CRISC & ITCA

Mr. Naveenkumar M S

Coordinator – CISA, CGEIT & CDPSE

Mr. Vijai K

Director – Academic Relations

Mr. Sampatkumar Krishnasamy

CONTENTS

ISACA
Bangalore Chapter

InfocITy
Auditor

Q4 - 2023

From The Desk Of The President

Dear Bangalore Chapter Members,

As we embark on this exciting new year, I want to extend my warmest greetings and share some thrilling news! 2024 promises to be a phenomenal year for ISACA Bangalore, overflowing with high energy, impactful initiatives, and a renewed commitment to empowering our members.

I'm incredibly proud to announce that, for the first time ever, our chapter has been chosen as the recipient of the prestigious 2024 ISACA Outstanding Chapter Achievement Award in the large chapter category! This is the highest chapter accolade, recognizing our dedication to exceeding service goals and actively supporting our local membership. This truly sets the bar high, and I commend each and every one of you for contributing to this remarkable achievement.

Serving as your president for the second term has been an immense privilege. Through in-person events, chapter office interactions, educational institution collaborations, and countless one-on-one conversations, I've gained invaluable insights into your needs and aspirations. This knowledge fuels our mission to provide exceptional services, resources, and guidance that equip you to navigate the ever-evolving challenges you face.

But our journey doesn't stop here. The excitement is just beginning! ISACA Global is committed to introducing several groundbreaking initiatives throughout the year:

- Privacy in Practice research: Get ready for cutting-edge insights into the latest global trends impacting the data privacy profession.
- Industry thought leadership: Expect a continuous stream of thought leadership on critical topics like AI, cybersecurity, and digital trust.
- Digital Trust Ecosystem Framework: Coming in March, this framework will empower organizations to build and maintain trusted relationships within the digital ecosystem. A new course and board briefing will accompany its release, along with a dedicated guide for AI implementation.
- ISACA 2024 Virtual Conference: Mark your calendars for February 20-22! This conference will be tailored to three global regions, offering valuable takeaways on emerging technologies and all aspects of our digital trust professional domains. Discounted rates are available, so join remotely for this enriching experience!
- Certification updates: ISACA's renowned CISA certification will be revamped to reflect the latest industry demands and knowledge requirements for information systems auditors. The Cybersecurity Audit Certificate will also be refreshed, ensuring our certifications remain at the forefront of the field.

ISACA Bangalore Chapter has already hit the ground running, hosting two packed Data Privacy Advisor and Privacy Practitioner training courses, followed by an IT Governance Control training, all happening right here in our chapter office. This is just the beginning of our commitment to providing you with the best possible learning and development opportunities.

As we navigate 2024 together, I wish each and every member a year filled with health, prosperity, and personal and professional fulfillment. I look forward to keeping you updated on all the exciting developments to come, and I have no doubt that together, we will achieve remarkable things.

Happy New Year, and let's make 2024 a year to remember!

Sincerely,
RAJASEKHARAN K R, CISM, CDPSE, CRISC®, PMP, ISO 27001 LA, ITIL (E), CSM, COBIT-5(F)

Message From the Vice President

Dear Members, Friends and Partners,

ISACA Bangalore chapter is delighted to announce the prestigious achievement of being awarded the Outstanding Chapter Achievement Award 2024 in the large Chapter Category worldwide.

Special thanks to all the EC teams since the inception of our Chapter without whose unwavering commitment and contributions such an achievement would not have been possible.

Serving as VP since 2022, I extend my sincere and heartfelt gratitude also to the members, industry leaders, academia, young professionals, and student volunteers who played a pivotal role in this success.

With a profound sense of resilience, accomplishment, and gratitude, I thank all of you who made it possible.

As the largest chapter in India, we remain committed to hosting training conferences, workshops, and seminars featuring expert speakers sharing the latest insights. Simultaneously, we strive to strengthen our connections with partners across sectors to enhance awareness of IT governance. Our Board of Directors prioritizes the interests of our members, and we anticipate continued enjoyment of the activities we offer.

We express gratitude for your ongoing support and eagerly anticipate your participation in our upcoming events.

Best Regards,
VIJAYAVANITHA S., CISA, CIA, MBA

Message From Secretary

Dear ISACA Bangalore Chapter Members,

I hope this email finds you all in good health and high spirits. My name is Deepak, and I am honored to address you as the newly appointed Secretary of the ISACA Bangalore Chapter. It is with great enthusiasm that I step into this role and embark on this journey alongside each and every one of you.

As your new Secretary, I am committed to upholding the values and objectives of our esteemed organization while also fostering an environment of collaboration, growth, and innovation within our chapter. With your support and participation, I am confident that we can achieve remarkable milestones together.

I would like to take this opportunity to express my gratitude to the outgoing Secretary for their dedication and hard work in leading our chapter. Their contributions have laid a solid foundation upon which we can build and thrive.

Moving forward, I am excited to announce some upcoming initiatives and events that we have planned for the benefit of our members. These include:

1. **Educational Workshops and Webinars:**
   Prepare for a series of engaging workshops and webinars exploring the latest in cybersecurity, cyber resilence, risk management, and governance. Renowned industry experts will guide us through these sessions, ensuring we stay abreast of emerging trends and best practices.

2. **Professional Development Opportunities:**
   Committing to lifelong learning, we'll be introducing initiatives like certification review courses and skill-building sessions. These programs aim to empower our members in their professional journey, equipping them with the skills needed in the dynamic field of information security and assurance.

3. **Networking Events:**
   Recognizing the value of networking, we plan to host virtual and in-person networking events (where feasible). These gatherings will provide a platform for members to exchange ideas, share experiences, and build valuable professional connections.

The enthusiasm for the opportunities ahead is contagious, and we eagerly anticipate your active involvement in these initiatives. Together, we'll make 2024 a year marked by growth, shared learning, and collective achievements.

Thank you for being an integral part of our ISACA Bangalore Chapter.

Best Regards,
DEEPAK BHASKARAN

Renewal of ISACA Membership for the year 2024

Warm Greetings from ISACA Bangalore Chapter!!!

We thank you for your continued support and commitment to professional excellence by earning one or more of ISACA Certifications.

Use your ISACA® membership and ISACA certification(s) as the platform for your growth by utilizing the opportunities for professional development. As you would have experienced, your ISACA membership and certification(s) increase your advancement opportunities by keeping you informed of standards and good practices in the fields that matter most to you and providing access to leading edge research and knowledge through Journals, Webinars, Blogs, ISACA e-library, local chapter events and many more.

Also, you are aware ISACA Bangalore Chapter provides significant benefits and local networking opportunities to its members. The chapter has been in the forefront and served its members in their quest for acquiring professional knowledge by conducting regular CPE Sessions, Webinars, Conferences and other professional development programs. At the chapter it is our endeavor to bring to the table the most relevant of the current topics and encourage active participation of members.

Visit www.isacabangalore.org for more information.

Please click below to renew *(login with your ISACA username and password to renew)*

http://www.isaca.org/renew

In case you need any assistance, please do not hesitate to reach out to Chapter Office at chapter@isacabangalore.org

For your information, the membership dues are indicated here below:

International Membership Dues:	**$135.00**
ISACA Bangalore Chapter Dues:	**$10.00**
Total Dues for 2024 membership renewal:	**US$ 145.00**

HURRY UP AND SAVE 15%

Time is running out to save 15% when you become an ISACA® professional member. Don't miss your chance to take advantage of globally-recognized training and professional development opportunities that can help you grow your skills, increase your earning power and get you noticed by employers.

DEEP SAVINGS.. DEEPER VALUE

ISACA members receive up to 25% OFF on exam registration, up to 30% off on exam prep materials, deep discounts on audit programs, 72+ hours of free CPE credits, online courses, career coaching, publications and more.

SAVE TODAY.. EARN TOMORROW

More than saving money, an ISACA membership empowers you to grow your knowledge, skills and professional network to increase your appeal with employers and your future earning potential.

Note: ***Apart from the above, certification maintenance dues may apply as per the certifications held.***

ISACA

Bangalore Chapter

To Register Scan the QR
or got to
http://tinyurl.com/2jp3ywta

CISA, CISM, CRISC, CDPSE, CGEIT

Online Review Classes

Fees (per course)
₹ 8,500 Members | ₹ 9,500 Non-members

Full Day: **9:30 am to 5:30 pm** IST live online via Zoom Platform and classroom option

Key features: Industry faculty, Official ISACA Presentations, Q&A discussion and more

ISACA 2024 OUTSTANDING CHAPTER ACHIEVEMENT AWARD

Recipient of the Outstanding Chapter Award

CISA	CISM	CRISC	CDPSE	CGEIT
Certified Information Systems Auditor	Certified Information Security Manager	Certified in Risk & Information Systems Control	Certified Data Privacy Solutions Engineer	Certified in the Governanceof Enterprise IT
5 Weekends	4 Weekends	4 Weekends	3 Weekends	4 Weekends
Domain 1 24-Feb Information Systems (IS) Auditing Process	Domain 1 16-Mar Information Security (IS) Governance	Domain 1 27-Apr Governance	Domain 1 14-Apr Privacy governance	Domain 1 30-Mar Governance of enterprise IT
Domain 2 25-Feb Governance and management of IT	Domain 2 17-Mar Information Risk Management	Domain 2 28-Apr IT risk assessment	Domain 2 20-Apr Privacy architecture	Domain 2 31-Mar IT resources
Domain 3 02-Mar IS Acquisition, Development, and Implementation	Domain 3 23-Mar IS Program Development and Management	Domain 3 04-May Risk response and reporting	Domain 3 21-Apr Data lifecycle	Domain 3 06-Apr Benefits realization
Domain 4 03-Mar Information systems operation and business resilience	Domain 4 24-Mar IS Incident Management	Domain 4 05-May Information technology and security		Domain 4 13-Apr Risk optimization
Domain 5 09-Mar Protection of information assets				

Why ISACA Bangalore Chapter ?

- The ISACA Bangalore chapter Instructors are well qualified to deliver top-notch training for exam preparation by using latest training techniques.
- Experienced CISOs and high-level professionals from prominent corporations share practical exercises w.r.t the content of Review manual.
- Checklists are provided to students to ensure sufficient coverage of key Concepts & Review Manual and well mapped Exam content.
- Exam Toppers are honoured every year in the Annual Karnataka conference of ISACA Bangalore Chapter.
- Employment references and vacancies are provided as a starting point and advice for advancing the successful students careers.

Queries: chapter@isacabangalore.org
certifcations@isacabangalore.org

☎ **080-4151 4331**
98865 08515

Recipient of the
Outstanding Chapter
Award 2024

ISACA
Bangalore Chapter

ONE IN TECH™
SheLeadsTech
2024

16 Mar 2024 | 9.30 – 5:00 pm

Celebrating International
Women's Day 2024

Grab your ***Sponsoring***
opportunity with

ISACA Bangalore Chapter

ISACA Bangalore Chapter
B10 Solus Jain Heights 1st Cross
JC Road Bangalore 560 002

☎ +91 98865 08515

✉ Chapter@isacabangalore.org

Recap of Newsletter Q4 - 2023

CPE Sessions:

1. Topic : "Self-Sovereign Identity - Time to liberate Data Subjects"
Speaker : Mr. Swarup Ghosh - Product Security Manager, MSN Pvt. Ltd.
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 9-Dec-2023 Time : 5:30 PM - 7:30 PM IST
Free Attendance : 2 CPE Credits offered

Speaker Profile:

Swarup Ghosh is an enthusiastic learner and active participant in the realm of digital security. Swarup Ghosh's proactive involvement in academic initiatives and international conferences reflects a passion for staying informed and contributing to advancements in cybersecurity. Eager to explore the intersections of technology, identity and privacy.

Swarup is poised to make meaningful contributions to the field, and he delivered a session for the following organizations:

- CMR University, MTech. program, Cyber Security Jagruti Divas
- International Cybersecurity Conference by Society General: Quantum Computing, Post-Quantum Cryptography
- International Cybersecurity Conference by the Society General

Topic Abstract:

Self-sovereign identity (SSI) is a form of digital identity that the user has complete control over. This means that the user decides who sees what information and when.

Digital identity is a user's online identification, similar to a physical identification card such as a passport or driver's license. A digital identity contains characteristics or attributes of the user.

With Self-Sovereign Identity, individuals can store their data to their devices and provide it for verification and transactions without the need to rely upon a central repository of data. With self-sovereign identity, users have complete control over how their personal information is kept and used.

2. Topic : "Navigating Compliance in a Multi-Cloud Environment"
Speaker : Mr. Mahesh Vastrad, Founder & MD - Agamya Cybertech
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 16-Dec-2023 Time : 5:30 PM - 7:30 PM IST
Free Attendance : 2 CPE Credits offered

Speaker Profile:

Mr. Mahesh Vastrad is a seasoned professional with a rich background in cybersecurity, audit, digital forensics, and risk management, over 6 years of experience in the field. Mr. Vastrad possesses a keen understanding of digital forensics, enabling him to investigate and analyze digital incidents with precision and thoroughness.

Also made significant contributions to education, conducting over 33 workshops that have reached and benefited 5000 plus students and police officers. His commitment to knowledge dissemination has played a vital role in empowering young professionals in the cybersecurity domain.

Topic Abstract:

In today's dynamic business landscape, many organizations are leveraging the benefits of multi-cloud environments to enhance flexibility and scalability. However, ensuring compliance across diverse cloud platforms is crucial for mitigating risks and meeting regulatory standards. The session will cover navigating multi-cloud compliance and why it requires a strategic and proactive approach. How to secure data, maintain consistency in policies, and adopt vigilant monitoring practices. How organizations can harness the full potential of multi-cloud environments while safeguarding against compliance risks

3. Topic : "ITGC Assessment Workshop"
Trainer : CA Narasimhan Elangovan - FCA, DipIFR (UK), CISA, CDPSE
Date : 2 & 3-Dec-2023 Time : 10:00 AM - 6:00 PM IST (6 Hours each day)
Total Hours : 12 hours
Hosted by : ISACA Bangalore Chapter

4. **Topic : "GDPR-DPDP Privacy Practitioner and Data Protection Officer"**
   Trainer : Mr. Kersi Porbunderwala
   Date : 8 to 10-Dec-2023
   Venue : Solus Jain Height, B10, 1st A Cross, J C Road, Opposite Poornima Theatre, Bengaluru, Karnataka - 560 002.

5. **Web Based Free Introductory Seminar on ISACA Certifications**
   Date : 18-Nov-2023
   Timings : 4.00 PM to 5.00 PM

Briefed about the CISA,CISM,CRISC,CDPSE and CGEIT Review classes by Mr. Vijai, Mr. Naveenkumar MS and Sampathkumar Krishnasamy of Directors about the usage of ISACA Certfications and benefit of doing for Job Opportunities in Various Software field to the Registered Participants through Zoom Platform.

Students Keenly Understand the usage of the Certfications and eagerly looking for the Upcoming Review classes from ISACA Bangalore Chapter.

40 Nos Participated and the session is concluded with good response from the Participants.

We are proud of the active and engaged community we have built at the ISACA Bangalore Chapter. These events are a testament to our commitment to providing our members with valuable learning and networking opportunities. We look forward to hosting even more exciting events in the months to come.

Stay tuned for upcoming announcements and event details!

The Digital Twin Advantage in Automotive Manufacturing Systems

- Karthik Trichur Sundaram & Divya Karthik

Digital twin technology has gained significant traction with the emergence of big data and the Internet of Things (IoT) and is now being utilized in many industries worldwide. A digital twin is a virtual model of a physical object designed to accurately reflect the object.

In digital twin technology, a physical object is outfitted with many sensors across different areas of functionality so that the sensors can effectively measure attributes of the physical object (e.g., temperature).[1] The sensors collect and relay data to the processing system, which applies the data to the digital copy, updating it in real time. With these data, simulations using artificial intelligence (AI) wand machine learning (ML) can be run on the virtual model to further study performance and help make decisions.[2]

The data allow for valuable insights that can be applied to the original physical object, improving its overall condition and performance.[3]

Virtual models are used by industries such as construction and automotive manufacturing to help identify which areas of performance manufacturers should focus on and what possible improvements can be made. For example, the construction industry effectively uses digital models of buildings and bridges to understand their structural integrity better and to pinpoint any issues. In addition, digital twin technology is used in complex projects such as the production of jet engines, aircraft and automobiles to improve the overall efficiency of the products.[4]

Digital twin technology using AI and ML in the automotive industry can enhance the overall design and efficiency of automotives products; however, these technologies pose cybersecurity risk. Therefore, it is essential to understand the mitigation measures organizations can take to protect themselves and their products.[5]

ML Algorithms in Digital Twin Technology

Digital twin technology uses AI, or more specifically, ML algorithms, to effectively analyze and assess the large amounts of data the sensors provide.[6] The aim of both AI and ML is development of intelligent programs that can handle complex tasks. ML algorithms are built on three major components: representation, evaluation and optimization. These components have requirements that must be fulfilled to generate an ML model and algorithm effectively. An ML-based twin of a production root cause analysis (RCA) process is intended to diagnose the root cause of a deficiency or anomaly found in the finished product or during the manufacturing process. It enables line managers to troubleshoot the most likely root causes based on the tool's predictions, identify the problem definitively, and implement corrective and preventative actions (CAPA) without spending too much time and effort searching through machine maintenance records, operator history, processes and IoT sensor inputs.[7] The goal is to minimize machine downtime and loss of production and enhance resource utilization.

Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations.

The Digital Twin Advantage in Automotive Manufacturing

The global digital twin technology market currently stands at US$9.5 billion and is expected to reach US$72.65 billion by the year 2032, at a robust compound annual growth rate (CAGR) of 22.6 percent from 2022 to 2032.[8] North America has the largest digital twin technology market share, with 40 percent.

The transportation and automotive sectors hold more than 15 percent of the market share due to growing demand for automotives. This could be explained by the growing adoption of electric vehicles (EVs) around the world.[9]

The advantages of digital twin technology are numerous, and its application can result in various advantages across industries. Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations. This testing revolves around the manufacturing of automotive vehicles and how their performance can be enhanced.[10] Digital twin technology can provide several benefits for automotive manufacturers including:

- Executing tests using the digital copy of the product or vehicle and simulating crash tests, autonomous driving and other scenarios to enable a better understanding of the various aspects of the vehicle that could be improved.[11]
- Testing with digital twin technology to confirm compliance with standards and automotive industry certifications such as International Automotive Task Force (IATF) 16949[12] and International Organization for Standardization (ISO) standards ISO 9001:2015 Quality management systems-Requirements,[13] ISO 14001:2015 Environmental management systems-Requirements with guidance for use,[14] and ISO 45001:2018 Occupational health and safety management systems-Requirements with guidance for use.[15]
- Improving overall customer satisfaction through the use of digital twin technology by using the sensors and the data digital twin technology provides, for example, to improve the performance, lifespan, safety levels and fuel efficiency of vehicles.[16]
- Enhancing the overall agility and resilience of the supply chain through digital twin technology. To form an understanding of what materials model home manufacturers can use for construction, for example, and what would benefit the product.[17]
- Understanding the overall energy consumption of a product and how it behaves - an electric vehicle for example, by developing a digital copy or model of the product and running the necessary simulations and design changes on the digital model to ensure that there are no issues. Test results and ML algorithms can aid in achieving a superior design with less energy consumption. Manufacturers can also gain an understanding of how they can improve the overall aerodynamics of a car and reduce the vehicle's weight.
- Assessing the effect on a vehicle of environmental factors such as temperature and humidity using predictive ML algorithms. Based on the data, different models can be tailored to the needs of every region and their geographies. Modifications or revisions to an important component or part can be published on the digital twin platform, allowing seamless collaboration by original equipment manufacturers (OEMs), automotive manufacturers, customers and service providers.

These benefits are the primary drivers of digital twin technology implementation in many manufacturing facilities across industries. The US-based automotive manufacturer Tesla uses digital twin technology in every vehicle it produces.[18] Thinkwik, the partner that developed Tesla's digital twin application, states that real-time mechanical issues at Tesla Motors, regardless of their magnitude, are fixed by simply downloading over-the-air (OTA) software updates.[19] It is important for manufacturers to continuously exchange relevant data with the vehicles they produce to improve the quality of their products. The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

Potential Risk of Digital Twin Technology

The adoption of evolving and emerging technologies to accelerate business growth inevitably creates an additional avenue of cyberrisk. Digital twins represent critical manufacturing assets that can directly affect an organization's bottom line. Though challenging, protecting digital assets is a key requirement organizations must meet when using digital twin technology. Although digital twin simulations can be used to monitor and track performance, they can also be configured to run real-life simulations to ensure that cybersecurity risk is mitigated.[20] However, securing digital twin operations, which are often hosted in the cloud, is another key challenge.

Digital twins represent physical systems, using additional inputs from sensors and controllers to provide a comprehensive summary for analysis. Although the physical assets may have protections such as microcontrollers or firewalls, digital twin representations can be vulnerable to security threats. Hackers can use cybersecurity threat techniques such as malware or spyware to control physical objects through digital twins, which could result in outages or major disasters. Digital twins may also represent objects that require intellectual property protection, such as semiconductors. If the digital twin is a blueprint of a piece of intellectual property, then hackers may be able to reverse-engineer and reproduce that property, bypassing the need for research and development of their own.

The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

The security of any organization is only as strong as its weakest link. If digital twin credentials are exposed, the organization may be compromised. This is because most digital twins are connected through application programming interfaces (APIs) to IoT and other systems. Hackers can use a weak digital twin to disrupt or bring down an entire organization in a short amount of time.

Recommended Risk Mitigation Techniques

IoT devices are generally less secure than traditional devices such as processors, so using them as sensors in a twin setup creates concerns. Because most organizations already have a cybersecurity framework that does not cater to digital twins or other emerging technologies, new generation digital projects often involve internal cybersecurity experts only on a need-to-know basis. However, cybersecurity experts within and outside the organization can be engaged on a dedicated basis with a proper budget at each stage of a digital twin project to mitigate security risk areas. Security leaders and chief information security officers can teach their employees about authentication, authorization, data integrity, data confidentiality and nonrepudiation using their standard cybersecurity framework. Every apparent and perceived threat should be documented.

An organization's cyberframework should have policies that help its security infrastructure to be scalable and cyberresilient to meet growing security needs. Static security solutions cannot provide adequate security.

The key to scalable security is constant adaptation and redesign-not just expensive security products and specialized security experts. The cyberframework should contain a planning strategy, streamlining, logic, up-to-date organizational policies, and security directives implemented by informed employees.

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal.

At both the interface level and the object level, digital twins should be protected with a zero-trust architecture. Multifactor authentication (MFA), microsegmentation and biometrics are additional layers of security that can help mitigate risk and provide returns on investment for secured organizational assets.

The use of ML algorithms for intrusion detection can help organizations identify and mitigate cybersecurity threats in a timely manner. However, it is imperative to train models using high-quality data sets to achieve successful intrusion detection. To build an attack model with high accuracy and low false positives, meaningful data collection and feature extraction are required. A digital twin-based security architecture can be effective for protecting industrial automation and control systems.[21] There are distinct security requirements for different components of the proposed architecture. It is advisable to synchronize clocks between the physical and digital twins at regular intervals to achieve active-state replication. Implementation of intrusion detection is critical to the entire architecture.

Conclusion

Digital twin simulation technologies are used by automotive manufacturers to gain an understanding of different aspects of the vehicle being designed. When applied to vehicle manufacturing systems, this technology can help reduce the cost of the vehicle, the level of carbon dioxide emissions, and fuel and maintenance costs, providing the manufacturer with a competitive advantage. Digital twins also allow manufacturers to improve the comfort, safety and efficiency of vehicles. ML algorithms can be used to develop digital models of a vehicle to test certain scenarios (e.g., vehicle crash, mechanical breakdown) and simulations to understand the various complexities and problems the product may encounter. They may also be able to improve the overall energy consumption of the vehicle, decrease air resistance, and make the vehicle more aerodynamic.

However, any organization that has digital twin capabilities is also at risk of cybersecurity threats. Digital twin projects should include cybersecurity experts at all stages. There should be enhanced security measures in place for all hybrid platforms and the network. Digital twins and their APIs should be tested for security vulnerabilities. Critical digital assets should be tested against hackers and disaster recovery mechanisms. A change agent can enforce security hygiene by implementing security measures such as zero trust architecture with MFA and additional security protection layers.

Digital twin assets security can be enhanced with ML. ML can analyze patterns in cybersecurity systems and learn from them to help prevent similar attacks and respond to changes in behavior. Real-time responses to active attacks can help cybersecurity teams be more proactive in preventing threats. Using ML-based cybersecurity systems to protect digital twin assets can reduce the time spent on routine tasks and enable organizations to utilize their resources more effectively.

Having an effective cybersecurity framework formalizes the subject matter expert's knowledge on anomaly detection. “If the framework has not seen a certain anomaly before, such as digital twin technology, a subject matter expert should analyze the collected data to provide further insights to be integrated into and improve the system,” said Efe Balta, a postdoctoral researcher at ETH Zurich.[22]

The expert can either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal. The technologies composing digital twinning such as IoT, industrial IoT, AI, ML, big data, simulation and cloud computing have been on a path of constant evolution; thus, it can be assumed that digital twin technology will continue to evolve in parallel to these technologies.

For more details - ISACA Journal/Issues/2023/Volume 4/The Digital Twin Advantage in Automotive Manufacturing Systems

PERILS OF ARTIFICIAL INTELLIGENCE (AI) IN INFORMATION SECURITY MANAGEMENT SYSTEM

- Akshaya Srivatsava

Abstract:

Artificial Intelligence has become a buzzword with increasing discussions at various top levels across the globe. It has grown in importance over the last couple of years and has recently taken the world by storm with introduction of ChatGPT. Rapid advancements in AI have also led to a global debate around the power and perils of AI in the field of Information Security Management System. There is a global demand for a risk-based approach to how people use / interact with this disruptive technology. Leaders across the globe believe that managing these risks is what will make or break organizations over the next decade. The main objective of the paper is to take a closer look at the dangers of AI in Information Security Management System and present some of the latest developments made to address challenges related to the adoption of these AI products.

Introduction:

Bell's law of computer classes formulated by Gordon Bell in 1972 describes that every 10 years, an entirely new class of computing emerges which is 10x smaller, cheaper, and faster. If this law is applied to today's world, we are already experiencing it via digital explosion with emerging technology like AI.

AI products nowadays are being used to improve business decisions, assist in automations of daily repetitive tasks, help in personalization, and deliver insights that were never seen before. Use of AI is growing rapidly all over the world and according to a recent report from Fortune Business Insights – AI industry / market is estimated to grow from 515.31 billion USD in 2023 to 2025.12 billion USD in 2030.[1]

How does AI impact Information Security?

With rise of numerous modern threats, obsolete security products can't offer the dynamic protection that can be provided by AI products and ML technologies. With use of such sophisticated technologies, businesses can create an enterprise security architecture which has a high-risk tolerance. They can have a tremendous impact on overall information security activities by enriching security events with data insights and more investigative opportunities. Few of the use cases where AI products are used:

- Identity and Access Management: AI tools can increase the accuracy for detection of access anomalies, detect user behaviour by looking at user login, location, activity details, target data to provide contextual insights and flag inappropriate events.

- Vulnerability management: Security Operation Centres (SOCs) can increase the use of AI products for active vulnerability and threat monitoring. This can improve SOC efficiencies and enable businesses to take a risk-based approach to vulnerability management.

- Endpoint discovery: AI products can be deployed on all enterprise assets to monitor suspicious activity and flag policy violations. It can also be used for anomaly detection and behaviour modelling.

- Case Management and Alert Management: Information security demands for an efficient case management and alert management systems. Having AI integrated in these processes can assist in processing of high volumes of data, classify and label information accurately and generate insights which was almost impossible with traditional tools.

- Enterprise data monitoring: Use of AI throughout the data lifecycle enhances the security team's capabilities to have a 360-degree view of data, adequately monitor it, provide analytics and identify patterns in voluminous amount of data for predictive analysis.

So, the biggest question remains - Is it as revolutionary as being perceived or is it a double-edged sword? - the devil might be in the details.

Risks associated with AI in Information Security Management System:

In a recent report by Gartner, 2023,[2] the risks around AI (large language model) were very well summarized. We can apply a similar threat landscape to comprehend the broader dangers presented by AI today in the world of information security.

Threat Vectors	Risk Category
Use by actors outside the organization	Cybersecurity risk Reputational risk
Ungoverned use by employees (Artificial Intelligence as a Service)	Information Security Risk Privacy Risk
Unintended consequences of enterprise use	Reputational Risk Legal and Regulatory Risk

1. **Use by actors outside the organization:**

There are a whole lot of dangers presented by use of AI tools by malicious actors. Using these AI tools, attackers can have more sophisticated and fine-tuned attacks and can even be done easily by least sophisticated attackers due to ease of availability of such tools. ChatGPT is the most popular of these tools now. Example: As per a recent article in The Register,[3] cybercriminals can use such tools to create convincing phishing emails and create spear phishing campaigns with higher chances of convincing a human brain (due to high quality of outputs). Attacker can also gather critical information of an organization to trigger a DDoS attack which then dents the 'availability' pillar of information security. Attackers can also impersonate chatbots and take organization brand or IP data which can cause reputational risk.

AI technology has a unique characteristic to adapt according to the environments hence can be used for execution of intelligent attacks and exploitation of unmitigated vulnerabilities leading to an increase in attack surface.

Hackers can also use AI technologies to weaponize malware to counter the existing cybersecurity solutions.[4] It can be used by the bad actors to understand the technology stack, integrations between different systems, communication protocols, and which systems are least protected. Subsequently, they can use to strengthen the stealth attacks.

Example: TaskRabbit was hacked compromising data of ~3.75 million users however analysts could not trace the attack. Stealth attacks are dangerous since external cyber attacker can secretly monitor the system communications, execute the attack and propagate the attack through the network and leave a system at will.

AI can facilitate such attacks and takeovers, and with the evolving technology, it will only lead to the creation of faster and more intelligent attacks.

2. <u>Ungoverned use by employees (Artificial Intelligence as a Service):</u>

It recently came to light that Google has asked its employees to use AI technologies like Chatgpt , Bing including its own Bard carefully for work. They have also asked their engineers to avoid using code generated from these platforms.[5] Companies like Apple, Amazon, Walmart, JP Morgan, Verizon , Accenture have also taken similar steps due to increase in instances where company information and confidential information such as code is being shared with chatbots. As per a recent report, Stack overflow banned use of ChatGPT and labelled it as 'harmful' due to code quality concerns.[6] These kind of scenarios present major risks around breach of data and confidentiality, exposure of client information along with privacy violations.

Example: Employees can input their organizational risk management strategy into a tool like ChatGPT to summarize the information for executive members. A bad actor can then query the tool, ask for risk and strategic priorities for the same company and then use it to their advantage to orchestrate an attack against the organization. Use of copyrighted materials as an input to AI models is already a legal grey area.

There are already instances such as Samsung banning the use of AI powered chatbots due to upload of sensitive information such as source code and transcripts of internal meetings by the employee to automate portions of their job.[7]

In a recent research done by Cyberhaven,[8] a data security company, it was noted that:

- 11% of data that the employees paste into ChatGPT is confidential.
- 4% of employees have already pasted sensitive data into it at least once.

Such ungoverned use of AI by employees can dent the 'confidentiality' pillar of information security.

3. <u>Unintended consequences of enterprise use:</u>

AI has error rate as well just like other technologies. As per a report from Brand Education,[9] error rate for AI is 23.31% in health care which is dangerous considering the high stakes involved in health care industry. Incomplete data input / unauthorized changes to datasets in AI model presents the risk of flawed results and unreliable outputs. An organization using such results can make decisions biased towards certain outcomes and can end up in financial loss / regulatory fines / reputational loss. This also dents the 'integrity' pillar of information security.

According to a survey by Forrester,[10] 50% of consumers feel frustrated with their interactions with the chatbots and 30% of the customers want to move their purchase to a different brand due to negative experiences. Hence, utilization of AI for the automation use case of customer support conversation is already proving to be harmful.

Not following disciplines in AI development can also lead to reputational risk. One such instance noted was when the shares of Google took a nosedive of 100 billion dollars after their new AI chatbot made a mistake.[11]

Datasets are the backbone of AI, but AI can also suffer from something known as information / data bias. This is considered as one of the hidden risks of AI. If the data is biased, the AI system and results will also be biased. AI products will always be as good as the data they are trained on. Relying on such results can lead to losses, fines and can risk a company's reputation. Furthermore, it can also expose a business to plagiarism and copyright infringement.

Example: Use of biased AI algorithms for hiring by HR teams can lead to nondiverse workforce

Over reliance on AI might also lead to lack of creativity and innovation in the workplace and such ethical considerations and data governance concerns are acting as a barrier for faster AI adoption.

<u>How should AI dangers be regulated - if at All?</u>

- Establish comprehensive regulations globally and locally that should govern the use and address various aspects of AI.
- Establish an AI risk assessment framework and conduct a comprehensive risk analysis to assess the potential impact of these risks to the organization. Some of the frameworks available in this area are NIST AI Risk Management Framework, BSA Framework, US Government Accountability Office (GAO) Framework etc.
- Development of the AI products needs to be controlled, self-regulated and should comply with local / state laws to ensure taking user's privacy,[12] security and anonymity into consideration.
- AI models needs to be transparent and explainable to help the users understand the data used for reaching the decisions, overview of algorithms utilized, and features of the model used for the decision making.
- Human error and insider threats are the biggest risk to AI systems. Appropriate training needs to be prioritized by the organization to create a well-informed workforce.
- Right data and models for the AI product needs to be selected. It needs to ensure that the data is relevant, diverse and unbiased.
- Continuous monitoring and auditing of AI products needs to be done to ensure that necessary interventions and escalations are done as and when needed.
- More investment needs to be done in research, development, and education in the field of AI.

<u>Recent Developments / News:</u>

- Rajeev Chandrasekhar, Minister of State for Electronics and Information technology for India recently mentioned that Digital Personal Data Protection Bill, 2022, and the proposed Digital India Act, 2023 will focus on user protection from emerging technologies like AI.
- Sam Altman founder and chief executive officer of OpenAI, the company that developed ChatGPT has demanded for a regulation to regulate AI development.
- On 26th January 2023, NIST released the AI Risk Management Framework (AI RMF 1.0) to manage risks to individuals, organizations and society due to use of AI .[13]
- An AIA (Artificial Intelligence Act) was recently approved by a majority vote in EU Parliament on 14 June, 2023.[14] The AIA aims to regulate artificial intelligence (AI) to ensure better conditions for the development and use of AI innovative technology and strengthening rules around data transparency and accountability.
- EU and US have plans to draft a voluntary AI code of conduct to address various risks associated with the technology.[15]

Conclusion:

In this work, a comprehensive review of dangers around AI in information security management system has been presented. Taking care of the risks associated with use of AI technology is crucial as more and more adoption of the technology happens. Al technology is not going anywhere but with great power comes great responsibility.

When it comes to AI in Information security management systems, all stakeholders play a key role in managing risks around the technology. While there are a list of perks AI offers, tech experts shouldn't ignore the risks involved. They need to look for ways to remove or reduce AI's potential risks and make its benefits more valuable.

The goal should be to start a dialogue on creating standards that will reduce the risk from use, misuse, and exploitation of technology. By establishing a robust risk framework, ethical implementation practises, continuous monitoring and appropriate training, organizations can effectively manage the dangers of AI related risks to information security.

Dangers around AI cannot be an afterthought and needs to be understood well and carefully regulated as we make a move towards higher adoption of such AI products / tools.

Bibliography

[1] Fortune Business Insights (April 2023) : Technology / Artificial Intelligence Market

[2] Gartner (10 March 2023): *What should audit know and do about ChatGPT and Large Language Models?* (Paid subscription required)

[3] Hardcastle Lyons, Jessica (11 January 2023): *AI-generated phishing emails just got much more convincing* , The Register

[4] Sharma, S (6 June 2023) : *ChatGPT creates mutating malware that evades detection by EDR* , CSO

[5] Kaustubh, Abhinav (15 June 2023) *: Google 'warns' employees about AI chatbots, including its own bard* , The Times of India

[6] Vigliarolo, B (5 December 2022) : *Stack Overflow Bans ChatGPT as 'Substantially Harmful' for Coding Issues* , The Register

[7] Ikeda, Scott (13 April 2023) : *Samsung Employees Fed Sensitive Data to ChatGPT While Using It to Check Code, Create Presentations*, CPO Magazine

[8] Coles, Cameron (18 June 2023) : *11% of data employees paste into ChatGPT is confidential* , Cyberhaven

[9] Brand Education (2 February 2022) : *AI's Error Rate Of 23.31% Unacceptable In Medicine: Why Medical Professionals Choose Human Transcribers*

[10] Press, Gil (1 February 2023) : *One Negative Chatbot Experience Drives Away 30% Of Customers*, Forbes

[11] Coulter, Martin and Bensinger, Greg (9 February 2023) :*Alphabet shares dive after Google AI chatbot Bard flubs answer in ad*, Reuters

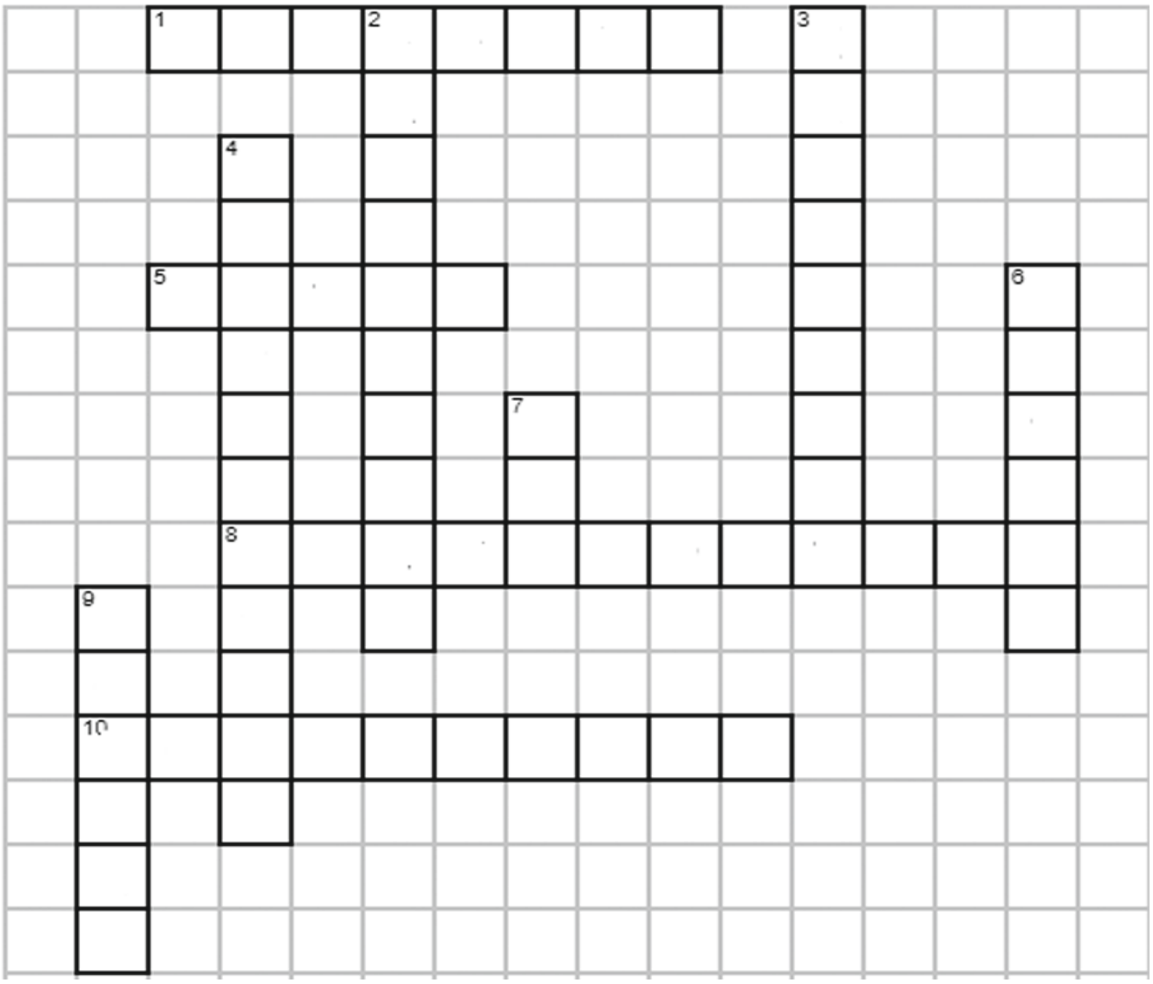
[12] Van Rijmenam, M. (17 February 2023) : *Privacy In the Age of AI: Risks, Challenges and Solutions*, The Digital Speaker

[13] National Institute of Standards and Technology (NIST) (January 2023): AI RMF

[14] The AI Act, "The Artificial Intelligence Act"

[15] The Strait Times (1 June 2023) : *EU, US to Draft Voluntary AI Code of Conduct*

CROSSLIMITS WITH CROSSWORDS



ACROSS	DOWN
1. 1 half of word "Seems way down" and second half is "artificial". (8 letter) 5. This acronym ensures safe internet browsing (4 letter) 8. You bite how much you can chew to avoid uncertainity (11 letter) 10. This allows applications to be more rapidly deployed, patched or scaled (10 letter)	2. Passwords are gone, these are new in town (11 letter) 3. This word first half "number invented by an Indian with Second half "belief" (9 letter) 4. This ensures optimized delivery when done with the provision of "Right to audit" (11 letter) 5. This format of Aadhaar is now accepted by RBI as preferred identifier (7 letter) 6. This acronym revolves around "Something you have" "Something you are" and "Something you know" (3 letter) 9. More efficient use of system resources in a cloud (6 letter)

Three lucky winners will be awarded Rs.500 gift voucher each.

All the responses will be sent to chapter manager email address (chapter@isacabangalore.org).The responses should contain the photo / scanned copy of the filled crossword, Member name, ISACA ID, email and contact phone number.

Last date for sending the crossword results is **March 10th, 2024.**

AGM 2023 - A Resounding Success!

Our Annual General Meeting (AGM) was held on October 28th, 2023, marking the first time ever that it was hosted at our very own chapter office. We are grateful to everyone who attended and participated in this momentous occasion. We also extend our sincere thanks to the nomination committee and to those who nominated to the new EC team. We are confident that the new team will lead the chapter to even greater heights.

Deep Dive into ITGC with In-Person Workshop

On December 2nd and 3rd, 2023, we organized an in-person IT Governance Control (ITGC) Assessment Workshop at the Bangalore Chapter office. Led by the esteemed CA Narasimhan FCA, DipIFR(UK), CISA, and CDPSE, the workshop provided valuable insights and practical guidance on conducting effective ITGC assessments.

Second batch of Certified Expert Practitioner (CEP) Training and third batch of DPO (Data Protection officer)

In collaboration with the e-compliance academy/EUGDPR institute and Mr. Kersi Porbunderwalla, and Mr. Atul Juvle, LLB General Counsel & Certified DPO, we hosted a Certified Expert Practitioner (CEP) & DPO training program on December 8th-10th, 2023. This program equipped participants with the knowledge and skills needed to excel in the field of data privacy and GDPR compliance.

Hackers work hard.
We work smart.

sentinelone.com

innspark

Explore.
Transform.
Fortify.

Innspark, a deep-tech solutions provider, offers out-of-the-box cybersecurity solutions to detect and address cyber incidents, threats, and attacks. In addition to enhanced visibility over an enterprise's security posture, our solutions deliver superior threat identification and response by leveraging the advanced analytical approaches of machine learning and artificial intelligence.

In-depth threat analysis, seamless deployment, improved threat hunting, enabling multiple integrations, revolutionary network security, and a cutting-edge unified security platform are our fundamental capabilities for advanced business protection.

Book Post

If undelivered please return to :

ISACA®
Bangalore Chapter

Solus Jain Heights, Unit No. : B10, 10th Floor
1st Cross, J C Road, Bangalore- 5600 02.
Ph. : 080-41514331/9886508515
Email: chapter@isacabangalore.org

Printed @ Cauvery Ent. ✆ 22128682

Chapter Reg No : 433/2002-2003