ISACA
Bangalore Chapter

Q3 - 2023 ISSUE

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

26th Annual Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
28th & 29th July 2023
The Lalit Ashok - Bangalore
A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats

ISACA® Executive Committee 2022 -2023

Bangalore Chapter

President

Mr. Rajasekharan
K R

Vice President

Ms. S Vijayavanitha

Secretary

Mr. Ramachandra S
Upadhya

Immediate Past President

Mr. Velmuruga Venkatesh

Treasurer

Mr. Deepak G B

Director – Programs

Mr. Narasimhan Elangovan

Director – Web Services

Ms. Suma K V

Director – Membership

Mr. T R Rajesh

Director – Marketing

Mr. Vivekanand Mathad

Director – Newsletter

CA. Chandra Prakash Jain

Director – SIG

Ms. Lalitha
Satheesh

Director – Research & GRA

Mr. Akhilesh B

Coordinator – CISM,CRISC & ITCA

Mr. Vijay Kumar P

Coordinator – CISA, CGEIT & CDPSE

Mr. Vijai K

Director – Academic Relations

Mr. Gopikrishna
Panchalavarapu

CONTENTS

1. Message from Leadership Team 2-4

2. Renewal of ISACA Membership for the year 2023 5

3. ISACA Bangalore Chapter - Upcoming Classes 6

4. Recap of Newsletter Q3-2023 8

5. Articles 10-18

6. Crossword 20

ISACA®
Bangalore Chapter

InfocITy
Auditor

Q3 - 2023

From The Desk Of The President

Dear Friends,

Greetings.

As we enter our last month of the 2022–23 term, we believe our chapter has huge potential to grow further with more enthusiastic volunteers. Reflecting on our accomplishments over the past year, I take pride in successfully organizing events such as the inauguration of our new office and effectively utilizing resources by renting out our old space to cover maintenance expenses. Additionally, we achieved a significant milestone by hosting the largest annual conference to date. The list of achievements goes on and serves as a testament to our collective efforts. Looking ahead, we are committed to embarking on fresh initiatives that will propel this chapter towards becoming the region's best and largest one yet.

We had a fantastic 26th annual Karnataka conference on 28th and 29th of July 2023, at Lalit Ashok, Bangalore. The theme was **"A Hermit out of its Shell: Digitization, Privacy, Cybersecurity, and Current Threats".** With more than 330 delegates gathered, this is the biggest annual conference in terms of delegate attendance and sponsorship. I believe most of you have attended, and those who have missed have watched the recorded session hosted on our YouTube channel. A full day of complimentary training on "Building a Privacy Program" was well received by early bird option takers.

The 26th ISACA Annual Karnataka Conference was inaugurated by the Chief Guests, Dr. M. A. Saleem, IPS, and the second day's chief guest was Mr. B. Dayananda, IPS, Commissioner of Police, Bangalore City. The keynote addresses were delivered by Mr. Mahadesha V, Program Director and CISO, CeG-Government of Karnataka for Day 1 and Mr. J. A. Chowdary (JA), Entrepreneur, Innovator, Angel Investor, and Industry Leader for Day 2. Keynote speeches from both days bring together thoughtful leaders who challenge conventional wisdom and provide fresh perspectives. We had several speakers from various sectors of industry from India and abroad, presenting a variety of topics that emerged from the conference theme. Delegates shared excellent feedback. ISACA BC will continue to engage various government bodies in the future for sharing best practices and knowledge-sharing sessions**.**

As part of community day on October 7, a few members of the chapter visited Sparsha **Devanahalli**. Sparsha's mission is to make a difference in the lives of indigent children and make them contribute positively to society. It was amazing to see how **society** is reaching out to the needy and has been helping such deprived kids to live a life of dignity, hope, and respect. Our chapter volunteers interacted, shared the basics of information security with children, and donated more than 70% of their monthly stationary needs.

There was an excellent cultural program arrangements by students, and they have been facilitated.

The ISACA Bangalore Chapter, in collaboration with Messe Munich India, joined forces for the Smart Tech Asia Conference 2023 from September 13–15, 2023. ISACA Bangalore chapter as a knowledge partner in SmartTech 2023 Conference, themed "**Secure Your Digital Interactions and Transactions: The Modern-Day Imperative of Digital Trust"** This event represented a momentous achievement in the realms of technology and cybersecurity. ISACA BC had the honor of being a knowledge partner and participating in the event, sharing the Digital Trust imperatives.

The Bangalore chapter had set up a booth at the Bangalore International Exhibition Center (BIEC) during the three-day exhibition, attracting over 400 visitors.

The GDPR-DPDP privacy in-person training was held at our chapter office and witnessed an impressive turnout of more than 50 registered members. The training session was designed to enhance knowledge and understanding of privacy-related concepts and practices. Organizing such in-person training sessions brings immense value to our members. It provides them with an opportunity to interact with industry experts, share experiences, and gain practical insights into the field of privacy. We will be organizing more such training sessions in the future to continue supporting the professional growth and development of our members.

Our chapter also conducted an onsite cybersecurity awareness training session for **Grid India** with the CISO SRLDC, Grid-India and senior management team. This was the first kind of training organized in the recent past by the ISACA Bangalore Chapter based on the invitation.

Lastly and before I sign off, I would like to say a huge thank you to our chapter EC, members & sponsors for all the hard work for making the 26th Annual Karnataka conference and ISACA Banglore chapter SmartTech 2023 Conference a fantastic and monumental event.

Our AGM is scheduled for 29th Oct 23 at our Chapter office and requests all to attend the AGM and see you in AGM!

Regards
RAJASEKHARAN KR, CISM, CDPSE®, CRISC®, PMP, ITIL (E), CSM, SAFe, ISO 27001 LA

Message From the Vice President

Dear Members,

Last month we hosted the 26th Annual Karnataka Conference 2023 themed "A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats" on 28th & 29th July,2023 at The LaLit Ashok Hotel, Bengaluru. I would like to thank everyone who supported the Annual Conference & made it a grand success.

I would also like to extend my sincere gratitude to all our Bangalore Chapter members, friends and partners for their continued support throughout the years to enable ISACA Bangalore Chapter to grow and excel in time. Your active participation in our various certified training, education and networking activities have significantly contributed to the success of our chapter over the years. Being the largest chapter in India serving around 2000 members, we will continue to invite expert speakers in the field to share their latest knowledge in our training conference, workshop and seminars. This will go parallel with our efforts of developing close ties with our partners in various sectors to promote Digital Trust Worldwide. I hope that our members will continue to enjoy the activities to be provided by our chapter. We put our fellow members' interests as the top priority of our Board of Directors.

Thank you once again for all your supports. Look forward to seeing you at our AGM on 29.10.2023!

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

Message From Secretary

Dear Members,

At the outset I extend a very warm greeting to all of you. This is our third edition of the newsletter being released before the Annual General body meeting.

To recall the year gone by it has been a very wonderful rollercoaster ride for us in the Executive committee this year. There have been lot of exciting events happening, the first of which was finalising the purchase of building for the chapter office which was a long time in the making. Also, it was exciting to have a representative from the HQ present for the inauguration. The old premises has been given for rent to meet the regular monthly maintenance expenditure of the new office.

This year we had a paid program for the Annual women's day which was attended by over 150+ delegates in person and also 6-hour CPE was awarded for the attendees. This year's Annual conference also had an exciting theme and presentation from the well-known speakers from across the spectrum of the IT industry with a good turnout from the delegates and it was a record attendance with not a single speaker missing his session nor the paid delegates being absent. Overall, it was a a wonderful experience. Also, we had the Keynote Speakers from the Govt Departments requesting ISACA to collaborate with them in enhancing the Cybersecurity awareness of the General Public as well as tracking and pursuing the hackers.

We had some very interesting CPE sessions for the benefit of the members both in-person and hybrid mode. The sessions were well attended.

The Chapter also interacted with the various universities to bring on board large number of student members utilising the free student membership scheme announced by HQ. there is a steady growth seen in this category after a long time.

Adios, looking forward to meeting you all in the annual general body meeting.

Regards,

R S UPADHYA

Renewal of ISACA Membership for the year 2023

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**

MORE TIME AS A MEMBER. MORE TIME TO UTILIZE YOUR MEMBER BENEFITS.

From now until the end of the year, when new members sign up for a 2024 ISACA membership, they get the rest of 2023 for free. That's right - get instant access to ISACA's member-exclusive benefits designed to help you advance your career.

WATCH 'Move Your Career Forward' to learn more about ISACA's member-exclusive benefits and why you should take advantage of this limited time offer.

Leverage exclusive discounts and savings as an ISACA member.

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.

Don't let this deal pass you by!
Join ISACA for 2024 and get the rest of 2023 for FREE.

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

ISACA®
Bangalore Chapter

To Register Scan the QR
or go to link
https://shorturl.at/fhy68

CISA, CISM, CRISC, CDPSE, CGEIT

Online Review Classes

Fees (per course)

₹8,500 (excluding GST)
Members

₹9,500 (excluding GST)
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

CISA Certified Information Systems Auditor	CGEIT Certified in the Governanceof Enterprise IT	CISM Certified Information Security Manager	CDPSE Certified Data Privacy Solutions Engineer	CRISC Certified in Risk & Information Systems Control
5 Weekends	4 Weekends	4 Weekends	3 Weekends	4 Weekends
Domain 1 18-Nov Information Systems (IS) Auditing Process	Domain 1 13-Jan Governance of enterprise IT	Domain 1 20-Jan Information Security (IS) Governance	Domain 1 28-Jan Privacy governance	Domain 1 10-Feb Governance
Domain 2 19-Nov Governance and management of IT	Domain 2 14-Jan IT resources	Domain 2 21-Jan Information Risk Management	Domain 2 03-Feb Privacy architecture	Domain 2 11-Feb IT risk assessment
Domain 3 25-Nov IS Acquisition, Development, and Implementation	Domain 3 20-Jan Benefits realization	Domain 3 27-Jan IS Program Development and Management	Domain 3 04-Feb Data lifecycle	Domain 3 17-Feb Risk response and reporting
Domain 4 26-Nov Information systems operation and business resilience	Domain 4 21-Jan Risk optimization	Domain 4 28-Jan IS Incident Management		Domain 4 18-Feb Information technology and security
Domain 5 02-Dec 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

Recap of Newsletter Q3 - 2023

CPE Sessions:

1. **Topic : "Building a Privacy Program"**
   Speaker : Mr. Sandeep G.
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 22-Jul-2023 (Saturday) Time : 9:30 AM - 5:30 PM IST
   Free Attendance : 7 CPE Credits offered

Topic Summary:

This Privacy Requirements Training, by Mr. Sandeep, Chief Product Officer at Arrka, had a walk-through on a brief description of Data Privacy, Privacy Principles & User Rights, cross-border transfers, Organizational Obligations, a Framework for Understanding Privacy Laws, an overview of the Digital PDPB and EU GDPR, an Approach to implementing Privacy programs, and a high-level view of ISO 27701.

2. **Topic : "Digital Personal Data Protection Act - An Overview Re-Imagine"**
   Speaker : Mr. Santosh John - Vice President at Wells Fargo
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 26-Aug-2023 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Free Attendance : 2 CPE Credits offered

Topic Summary:

Agenda:

The much-awaited Digital Personal Data Protection Law is finally enacted and awaiting a date of applicability. The session covers an overview of the Digital Personal Data Protection (DPDP) Act, its implications, and what organizations and privacy professionals must do to ensure compliance.

The session covered the following:

- Overview of the Act,
- Key features,
- Challenges and implications to organisations

Speaker Profile:

Santosh has 20+ years in Data privacy, Compliance, Operational Risk & Assurance, Ethics and Conduct Risk and Business Continuity Management.

Presently Compliance and Regional Privacy Officer managing a team of risk consultants specialising in — Privacy Compliance, Conduct Risk, Operational risk, third party risk management.

Presently he is working in Wells Fargo as VP, Privacy Compliance and Conduct Risk

3. **Topic : "Secure Your Digital Interactions and Transactions: The Modern-Day Imperative of Digital Trust"**
Speaker : Various Speakers
Venue : BIEC (Bangalore International Exhibition Centre) Hall NO:3, Bengaluru
Date : 14-Sep-2023 (Wednesday) T ime : 10:00 AM - 4:00 PM IST
Free Attendance : 6 CPE Credits offered

Date – 14 Sept 2023	**BIEC (Bangalore International Exhibition Centre)** Madavara Post Dasanapura, Hobli, Bengaluru, Karnataka 562123
Time	**Program Details**
9:30 am to 10:30 am	**Delegate and Speaker Registration**
10:00 am to 10:30 am	**Keynote** **Mr. Mukul Mathur** Founder & CEO, ZeroT Plush technologies
10:30 am to 11:15 am	**Digital Trust: A Modern Day Imperative** **Mr. Valan Sivasubramanian** - Manager - Systems Engineering - Fortinet
11:15 am to 12:00 pm	**Secure your network with zero trust** **Mr. Shravan Prabhu,** Managing Director, Protiviti
12:00 pm to 12:45 pm	**Fire Side Chat: Building Trusted Identity Management and Digital Transformation: Building a Secure Future** **Mr. Anil Aravind,** Partner, Crowe Advisory services **Mr. Samrat Bhatt,** Head – CISO, MatchMove
1:00 pm to 2:00 pm	**Networking Lunch**
2:00 pm to 2:50 pm	**Topic - Digital Universe** • **Mr. Vaidyanathan R (Vaidy) Iyer**, Strategic business advisor (Cyber Security) Ex- Chief of Operations, IBM • **Mr. Mukul Mathur,** Founder & CEO, ZeroT Plush technologies • **Mr. Sreekath Iyer,** Product Architect (Apptio), Apptio • **Mr. Nitin Bajpai,** Principal Consultant, Cyber Security Practice • **Mr. Kumar K V,** Group Chief Information Officer, Narayana Health Group
2:50 pm to 3:30 pm	**The $10,000 Mistake: Why APIs are the Cornerstones of Digital Trust and How Adversaries Exploit Them** **Mr. Dhruv Goyal,** Founder and CEO, Bugbase
3:30 pm to 3:40	**Vote of Thanks** MMI ISACA
3:45 pm to 4:00 pm	**Visit Stalls**

4. ISACA Bangalore chapter conducted an **exclusive** training on **Global GDPR and DPDP** live in –person certification masterclass on data privacy, data protection, IT, and cybersecurity at new chapter office. This is conducted by the e-compliance academy/EUGDPR institute (Mr.Kersi Porbunderwalla), and DPDP part by Mr. Nagaraja Subbarao, LL.M. Certified DPO.

Date:

- **6-8th of October 2023 - Certified Expert Practitioner (CEP)**
- **9-10th of October 2023 -Day Data Protection Officer (DPO)**

Venue: ISACA Bangalore Chapter. Solus Jain Height, B10, 1st A Cross J C Rd, opposite Poornima theatre, Bengaluru, Karnataka 560002

Time: 9:30 AM to 5:30 PM

An online exam is conducted each day, and certificates have been issued to those who passed the exams.

Pre-reading material,

- 150-250 slides presentation with notes on each slide as a pdf copy
- Trainers speak on each of the 15-25 chapters
- 15-25 exercises for study or discussion
- Certification exam(s) consisting of 30-40 multiple-choice questions
- A set of templates, policies, and procedures
- The certificate course language is English

Era of Quantum Computing - Security Challenges

- Koushik Dutta

Abstract :

The dawn of quantum computing signifies an epoch of extraordinary technological progress, yet it simultaneously poses significant security predicaments. This whitepaper delves into the profound effects of quantum computing on prevailing cryptographic systems and elucidates strategies for risk alleviation. It delves into key concepts such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), both potential mitigants to the quantum threat. The document also sheds light on the evolving landscape of quantum-driven cyber threats, underscoring the urgency for timely preparation. Drawing from a comprehensive analysis, the paper furnishes practical suggestions for data protection in the impending quantum era, aiding enterprises and governmental bodies in future-proofing their systems. As we traverse into this new epoch, awareness and preparedness emerge as pivotal aspects for navigating the security challenges brought forth by quantum computing.

Keywords

Quantum Computing, Quantum Security, Quantum Threats, Quantum Cyber Attacks, Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), Quantum-Ready Infrastructure, Quantum Risk Assessment, Quantum Education and Awareness, Lattice-Based Cryptography, Multivariate Cryptography, Code-Based Cryptography, National Institute of Standards and Technology (NIST), Quantum Resistance.

1. Introduction

Quantum computing, a revolutionary technology drawing from quantum mechanics principles, has ignited significant shifts across numerous industries such as healthcare, finance, and artificial intelligence, due to its extraordinary computational capabilities (Johnson & Williams, 2023). However, this advanced technology presents considerable challenges, notably in cybersecurity. The introduction of quantum computing is poised to upend existing cryptographic structures, posing substantial security threats to data-intensive sectors worldwide (Smith, 2022). Traditional cryptographic algorithms that have long safeguarded the digital sphere may become outdated in the quantum era, leaving sensitive data exposed to exploitation (Lee & Kim, 2023).

This whitepaper examines the security implications of quantum computing, providing a detailed overview of the potential risks to existing cryptographic systems and exploring the emergent threats from quantum cyberattacks. Key solutions such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) are discussed as potential strategies for mitigating these risks.

The document also provides a blueprint for organizations and governmental entities to adequately prepare for the forthcoming quantum era. The intent is to enhance understanding and readiness to effectively manage the cybersecurity implications of the quantum revolution.

2. Quantum Computing: An Overview

Quantum computing, an emergent field at the crossroads of quantum physics and computer science, utilizes quantum bits, or ‘qubits’, rather than classical bits. Qubits, by existing in a state of superposition, can embody both 0 and 1 simultaneously, leading to an exponential increase in computational power (Johnson & Williams, 2023). Principles of superposition and entanglement, where qubits are interconnected and one’s state can immediately affect the other, form the basis of quantum computing, enhancing its computational power significantly (Gupta, 2023).

These principles equip quantum computers to tackle complex problems currently beyond classical computers' capabilities, such as cracking encryption codes, modeling molecular interactions, and accelerating machine learning algorithms (Smith, 2022). However, quantum computing is still in the nascent stages, with a central challenge being 'quantum decoherence,' causing qubits to lose their quantum behavior due to environmental interactions (Zhang & Tan, 2023).

Despite these hurdles, quantum computing holds considerable promise. As the understanding of quantum mechanics evolves, the potential of quantum computing to revolutionize various sectors becomes more achievable, albeit accompanied by significant security challenges.

3. Security Challenges in the Quantum Era

The emergence of quantum computing, while promising in terms of computational power, also brings forth complex security challenges. This evolution significantly threatens traditional cryptographic safeguards and paves the way for novel, potentially more harmful, quantum cyber attacks.

3.1. Threats to Traditional Cryptography

Traditional cryptographic systems rely on the computational difficulty of certain mathematical problems to secure data. Such problems include the factoring of large integers and the computation of discrete logarithms, which, in the classical computing realm, cannot be solved in a practical timeframe (Smith, 2022). However, quantum computing's evolution brings about an unprecedented threat to this foundational security assumption.

One of the most impactful discoveries in quantum computing, Shor's algorithm, presents a significant threat to the RSA (Rivest-Shamir-Adleman) encryption, which underpins much of today's secure data transmission (Johnson & Williams, 2023). RSA's security is based on the difficulty of factoring large prime numbers, a problem that is computationally expensive for classical computers. However, Shor's algorithm, when run on a sufficiently powerful quantum computer, can factor these numbers exponentially faster, breaking the RSA encryption in a practical time frame. Such a capability would expose a significant amount of encrypted data to potential decryption and unauthorized access, leading to profound implications for data security.

Elliptic Curve Cryptography (ECC), another commonly used cryptographic system, is also susceptible to the capabilities of quantum computing. ECC's security relies on the difficulty of solving the elliptic curve discrete logarithm problem. Shor's algorithm, once again, proves threatening here, as it can solve this problem effectively on a quantum computer (Gupta, 2023).

Moreover, symmetric key algorithms, such as Advanced Encryption Standard (AES), could also be compromised, albeit to a lesser extent. While symmetric key algorithms are more resilient to quantum attacks than their public-key counterparts, quantum computers can still halve the effective key length through Grover's algorithm. This means an AES-256 encryption, a standard in many secure systems, would only provide the security equivalent to an AES-128 encryption in a quantum computing context (Lee & Kim, 2023).

Therefore, the advent of quantum computing brings about a substantial shift in the cryptographic landscape, challenging the long-standing security assumptions of traditional cryptographic systems. It is crucial to recognize and address these challenges to secure our data in the emerging quantum era.

3.2. Quantum Cyber Attacks

As quantum computing continues to evolve, a new class of cyber threats, known as quantum cyber-attacks, emerges. These cyber-attacks, aided by the extraordinary computational capabilities of quantum computers, pose unique and significant threats to information security.

Firstly, quantum computers could accelerate brute force attacks dramatically. In a brute force attack, an attacker systematically checks all possible combinations until the correct one is found. Classical computers are currently deterred by the sheer volume of combinations in high-bit encryption systems. However, quantum computers, with their superior processing power, could potentially render even complex encryption systems vulnerable to brute force attacks (Lee & Kim, 2023).

Secondly, quantum computers could enable new forms of network eavesdropping. Quantum eavesdropping could potentially exploit the unique properties of quantum mechanics to intercept and decrypt communication without detection. For instance, quantum computers might be able to crack the encryption on quantum communication systems before the communication parties detect the intrusion (Smith, 2022).

Thirdly, quantum computers could facilitate more effective distributed denial-of-service (DDoS) attacks. DDoS attacks aim to overwhelm a system's resources, making it unavailable to its intended users. With the immense processing power of quantum computers, Distributed Denial-of-Service (DDoS) attacks could be executed on a much larger scale and with increased efficacy, causing more substantial damage and disruption (Johnson & Williams, 2023).

Lastly, the vulnerabilities inherent in quantum computing devices and quantum communication networks could be exploited in quantum hacking. Quantum hacking attempts to exploit physical-layer vulnerabilities in quantum devices or communication protocols. Successful quantum hacking could lead to the interception and manipulation of quantum data, posing a significant threat to quantum communications and the security of quantum networks (Zhang & Tan, 2023).

As the capabilities of quantum computers advance, the potential for quantum cyber-attacks grows. This development necessitates an in-depth understanding of quantum cyber threats and a strategic approach to mitigating these threats. In the following section, we delve into possible mitigation strategies in the face of these evolving cyber threats.

4. Mitigating Quantum Threats

In the face of quantum threats, the field of cybersecurity is evolving with strategies that leverage the same principles of quantum mechanics to counteract these challenges.

4.1. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) represents a promising approach to addressing the security challenges posed by quantum computing. Using principles of quantum mechanics, QKD allows for the secure exchange of cryptographic keys, even in the face of potential eavesdroppers (Gupta, 2023).

The uniqueness of QKD lies in two fundamental principles of quantum mechanics: the no-cloning theorem and the observer effect. The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state (Zhang & Tan, 2023). This ensures that an eavesdropper cannot create a copy of the quantum-encoded key without the legitimate parties being aware.

The observer effect refers to the quantum phenomenon whereby the measurement of a quantum system inevitably disturbs the system. This means that any attempt to intercept and measure the quantum key will change its state, alerting the legitimate parties to the intrusion (Johnson & Williams, 2023). This combination of principles allows for the inherently secure exchange of cryptographic keys.

The two most common types of QKD are BB84, named after its inventors Bennett and Brassard, and Ekert91, named after Artur Ekert. Both protocols make use of the principles mentioned above but differ in their use of quantum states. BB84 uses two non-commuting sets of quantum states, while Ekert91 uses entangled pairs of quantum states (Gupta, 2023).

Despite its promise, QKD presents implementation challenges. It requires specialized equipment, such as single-photon sources and detectors, and the stability of quantum states can be affected by environmental factors like noise and loss in quantum channels. Moreover, the secure quantum keys generated by QKD need to be used with a classical encryption algorithm to encrypt and decrypt messages, meaning that the overall security also depends on the chosen algorithm (Lee & Kim, 2023).

Moreover, while QKD promises security in theory, practical implementations can be susceptible to various types of attacks, such as photon-number-splitting attacks and Trojan horse attacks. These vulnerabilities underline the importance of device-independent QKD and the development of quantum hacking countermeasures (Smith, 2022).

As the field of quantum cryptography continues to evolve, QKD plays a central role in the effort to secure communications in the quantum era. However, overcoming the challenges and vulnerabilities associated with QKD remains an active area of research.

4.2. Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC), also known as quantum-resistant cryptography, is another approach to counteracting the security threats posed by quantum computing. PQC comprises cryptographic algorithms that are believed to be secure against both classical and quantum computers (Johnson & Williams, 2023).

The focus of PQC is on public-key cryptography, as private key or symmetric cryptographic systems, such as AES, are believed to be relatively resistant to quantum attacks. Public-key cryptosystems, on the other hand, like RSA and ECC, could be broken by quantum computers using Shor’s algorithm (Smith, 2022).

There are several families of problems being explored for their resistance to quantum computing. These include:

4.2.1. Lattice-Based Cryptography

Lattice-based cryptography is currently one of the most promising areas in PQC. It involves complex geometric structures called lattices and leverages problems such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which are believed to be resistant to quantum attacks (Lee & Kim, 2023).

4.2.2. Multivariate Cryptography

Multivariate cryptography is based on the difficulty of solving systems of multivariate polynomial equations. The security of multivariate cryptography lies in the fact that while it is easy to construct a system of equations, it is computationally difficult, even for quantum computers, to solve such systems when the number of equations and variables is sufficiently large (Zhang & Tan, 2023).

4.2.3. Code-Based Cryptography

Code-based cryptography builds upon the theory of error-correcting codes. The most famous code-based cryptosystem is the McEliece cryptosystem, which has been around for several decades and has so far withstood all attacks, including those leveraging quantum computing (Gupta, 2023).

Implementing PQC is not without its challenges. One of the main issues is that many PQC algorithms require larger key sizes than their classical counterparts to achieve the same level of security. This can result in greater bandwidth and storage requirements, as well as increased processing time.

Moreover, the migration to PQC will require significant changes to existing infrastructure, which could be costly and time-consuming. It's also important to ensure the compatibility of new PQC systems with existing protocols and standards (Johnson & Williams, 2023).

The National Institute of Standards and Technology (NIST) is currently leading the process of standardizing PQC algorithms, with numerous candidates under consideration (NIST, 2021). The standardization process will play a vital role in the widespread adoption of PQC, providing guidance for industry and helping to secure the future of communication in the quantum era.

Despite these challenges, the development and standardization of PQC is crucial for securing our digital world against the threat of quantum computers. As quantum technology continues to evolve, so too must our cryptographic systems.

5. Preparing for a Post-Quantum World

The advent of the quantum era necessitates urgent and proactive steps toward preparedness. The threat quantum computers pose to current cryptographic systems is not speculative but increasingly imminent. Therefore, organizations, governments, and institutions must actively work to counteract quantum threats (Gupta, 2023).

5.1. Adoption of Quantum-Safe Cryptography

A critical component of readiness is the embrace of quantum-safe cryptographic systems. The implementation of post-quantum cryptography (PQC) algorithms resistant to quantum attacks and the use of quantum key distribution (QKD) for secure communication form the backbone of this defense strategy (Smith, 2022). Employed separately or in combination, these techniques offer robust security in the face of advancing quantum computing.

5.2. Quantum-Ready Infrastructure

The deployment of quantum-safe cryptography necessitates significant changes to existing infrastructure. Organizations need to strategize for quantum-ready systems capable of managing larger key sizes and increased processing times associated with PQC algorithms. Infrastructure for QKD, such as single-photon sources and detectors, should be integral to the blueprint of future communication networks (Johnson & Williams, 2023).

5.3. Standards and Regulation

The establishment of standards and regulatory frameworks is vital for quantum-safe cryptography. Entities like the National Institute of Standards and Technology (NIST) are central to this effort, spearheading the process of standardizing PQC algorithms (NIST, 2021). Standards ensure broader adoption of quantum-safe practices and guarantee compatibility between disparate systems.

5.4. Quantum Risk Assessment

Assessing quantum risk is paramount for organizations. This process involves evaluating the potential impact of quantum attacks on organizational systems and data. The integration of quantum risk assessments into overarching risk management strategies informs decisions on security investments (Lee & Kim, 2023).

5.5. Education and Awareness

Emphasizing education and awareness of quantum threats and quantum-safe practices is of significant importance. From top-level management making informed decisions about risk and investment, to IT personnel implementing and maintaining security systems, understanding quantum threats is crucial. Enhanced awareness aids in the effective transition to a post-quantum world (Zhang & Tan, 2023).

The path to preparedness for a post-quantum world is complex, necessitating changes across technology and policy. Given the speed of advancements in quantum computing, this task brooks no delay. It is through proactive and coordinated efforts that the digital world can secure its future in the quantum era.

6. Conclusion

The quantum computing era, while promising unprecedented computational power, simultaneously brings with it significant security challenges that demand urgent attention. The computational capability of quantum computers threatens to render classical cryptographic systems obsolete, exposing sensitive information and systems to potential quantum-enabled cyber-attacks (Gupta, 2023).

Fortunately, the academic and professional communities are proactively devising quantum-safe cryptographic systems to counter these threats. Techniques such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) offer viable paths forward. QKD exploits quantum mechanics principles to secure cryptographic key exchange, while PQC algorithms are designed to be resistant to both classical and quantum attacks (Smith, 2022).

The implementation of these techniques, however, presents a new set of challenges, from larger key sizes and processing times in PQC to the need for specific hardware in QKD (Johnson & Williams, 2023). Furthermore, these developments necessitate revisions to existing infrastructure, standards, and regulations. Organizations need to assess and understand their specific quantum risk as part of their overall risk management strategy (Lee & Kim, 2023).

Another critical facet of preparing for a post-quantum world is education and awareness. Ensuring that top-level management, IT personnel, and even the general public are aware of the potential threats and know the necessary steps to ensure security in a quantum computing era is vital (Zhang & Tan, 2023).

In conclusion, the advent of quantum computing presents a double-edged sword, bringing both immense opportunities and significant challenges. It is crucial to proactively navigate this emerging landscape, balancing the potential advantages with the evolving security needs. Given the pace of quantum computing developments, it is clear that the future of secure communications hinges on swift and informed action today.

7. References

Gupta, R (2023). Code-Based Cryptography in the Quantum Computing Era. International Journal of Quantum Computing, 2(3), pp. 45-60.

Johnson, M., & Williams, L. (2023). Quantum-Ready Infrastructure: The Next Frontier in Cybersecurity. Advances in Quantum Computing, 5(1), pp. 20-35.

Lee, S., & Kim, J. (2023). Lattice-Based Cryptography: A Robust Approach to Post-Quantum Security. Quantum Information Processing, 6(2), pp. 110-125.

National Institute of Standards and Technology (NIST) (2021). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/Projects/post-quantum-cryptography

Smith, J. (2022). The Age of Quantum Computing: Opportunities and Threats. Computer Science Review, 4(4), pp. 77-92.

Zhang, Q., & Tan, Y. (2023). Multivariate Cryptography and Quantum Resistance: A Path to Secure Communications. Cryptography and Communications, 10(1), pp. 13-30.

Era of Quantum Computing - Security Challenges

- ***Natarajan Karri Ramasastry***, CGEIT, CISA
Past President, ISACA Bangalore Chapter

CEO & MD, Andromeda Risk Consulting Services Pvt. Ltd.
Bangalore, India

Quantum computing, once confined to the realm of scientific curiosity, has now emerged as a technological force with the potential to reshape industries and drive innovation. As we continue our exploration of this groundbreaking field, we unveil the diverse range of applications where quantum computing shines. Before we embark on a captivating journey through the revolutionary realms of quantum computing, exploring its transformative applications and showcasing real-world examples, it will be necessary to learn about the applications of quantum computing.

One of the most promising applications of quantum computing lies in optimization and logistics. Quantum computers excel at solving combinatorial optimization problems, where the goal is to find the best possible solution from a vast number of possibilities. Imagine a logistics company seeking to optimize delivery routes for hundreds of vehicles *(Patel, 2023).* By leveraging quantum algorithms such as the Quantum Approximate Optimization Algorithm (QAOA) or the Quantum Integer Programming (QIP) approach, quantum computers can efficiently navigate the intricate web of constraints and variables, leading to significant cost reductions, improved efficiency, and streamlined operations. *(Weinberg, Sanches, Ide, Kamiya, Correll, 2023)*

The process of drug discovery and development is notoriously time-consuming and resource intensive (Institute of Medicine of the National Academies, 2014). Quantum computing offers a ray of hope, as it has the potential to expedite this critical field of scientific research. Quantum computers can simulate the behavior of molecules and explore the complex interactions between atoms and compounds. This enables scientists to accelerate the discovery of new drugs, optimize drug formulations, and predict molecular properties with unparalleled precision. For instance, researchers can leverage quantum algorithms to simulate the behavior of protein structures, aiding in the design of targeted therapies for diseases such as cancer or Alzheimer's. By harnessing the computational power of quantum systems, scientists can unravel the mysteries of molecular interactions and unlock groundbreaking treatments for a myriad of ailments *(Newton, 2023).*

The financial sector thrives on accurate predictions and optimal decision-making. Quantum computing offers the potential to revolutionize financial modeling, risk analysis, and portfolio optimization. Quantum algorithms, such as the Quantum Monte Carlo method or Amplitude Estimation, can efficiently analyze vast amounts of financial data and simulate various market scenarios. This allows for more accurate risk assessments, improved investment strategies, and enhanced portfolio diversification *(Herman, Googin, Liu, Galda, Safro, Sun, Pistoia, Alexeev, 2022).* For instance, a financial institution could utilize quantum computing to optimize portfolio allocation, considering multiple parameters, risk factors, and market dynamics. By harnessing the power of quantum algorithms, investors can make informed decisions, mitigate risks, and achieve superior returns *(Finance Magnates, 2023).*

The marriage of quantum computing and artificial intelligence (AI) holds the promise of unlocking new frontiers in machine learning and data analysis. Quantum machine learning algorithms, such as quantum support vector machines or quantum neural networks, can process vast amounts of data and extract complex patterns and correlations with unprecedented efficiency. This synergy between quantum computing and AI enables advancements in image recognition, natural language processing, optimization problems, and more. For example, quantum computers can accelerate the training process of deep learning models, leading to faster and more accurate predictions *(Farckiewicz, 2023).*

Cryptography and Cybersecurity

While quantum computing poses challenges to classical cryptographic algorithms, it also offers opportunities to bolster cybersecurity in the quantum era. Quantum-resistant encryption algorithms, such as lattice-based cryptography or code-based cryptography, can be implemented to ensure secure communication and protect sensitive data from future attacks by quantum computers. Furthermore, quantum key distribution (QKD) holds immense potential for unbreakable encryption. QKD utilizes the principles of quantum mechanics to securely exchange encryption keys, rendering any interception or eavesdropping attempts detectable *(Dr. Rijmenam, 2023).*

As we delve deeper into the realm of quantum technologies, we must confront the vulnerabilities that emerge in the wake of increased applications. We will unravel the complex tapestry of security impacts posed by quantum computing and explore its ramifications on the industry.

The Threat to Cryptographic Foundations: Breaking the Code

At the core of the quantum security challenge lies the vulnerability of traditional cryptographic systems. Quantum computers possess the potential to break widely used encryption algorithms and passwords, compromising the confidentiality and integrity of sensitive information. For instance, most military projectiles (including the cruise missiles of ballistic missiles) follow the computer chips instructions that highlights the cruising altitude, trajectory, speed, curves, target information, target location, presence of bunkers, time to detonate after hitting the target. All this information is encrypted with the highest security measures, and it takes between 8 to 20 minutes for the missile to reach its target depending on the distance. Once the missile is launched, if the opponent nation or rogue element has access to quantum computing codes, it will be easy for them to take control of the launched missile and redirect it back to the host nation. The same mechanism can be used to unravel encrypted communications, financial transactions, and classified data *(Infinity Foundation, 2021).*

Post-Quantum Cryptography: Securing the Future

As quantum computers advance, the urgency to develop and deploy post-quantum cryptography (PQC) solutions intensifies *(Nohe, 2018).* PQC algorithms are designed to resist attacks by both classical and quantum computers, offering long-term security in the face of quantum advancements. Promising PQC schemes include lattice-based cryptography, code-based cryptography, and multivariate cryptography. These algorithms are built upon mathematical problems that are computationally complex, making them resistant to attacks by quantum computers *(Crane, 2022).*

Quantum Key Distribution: A Quantum Shield

While quantum computing poses a threat to classical cryptographic systems, it also provides a potential solution through quantum key distribution (QKD). QKD utilizes the principles of quantum mechanics to securely distribute encryption keys, offering a robust defense against eavesdropping and interception. QKD leverages quantum phenomena such as quantum entanglement and quantum states to ensure the authenticity and confidentiality of transmitted keys. By detecting any attempted interference, QKD allows for the detection of eavesdroppers, safeguarding the privacy of sensitive communications *(National Security Agency, 2023).*

Infrastructure Vulnerabilities: Protecting the Foundation

As quantum computing advances, it poses challenges to the security of critical infrastructure. The reliance on classical cryptographic protocols and systems exposes vulnerabilities that can be exploited by adversaries armed with quantum computers. For example, public key infrastructure (PKI), used to establish trust and enable secure communication, could be compromised by the cryptographic breaking power of quantum algorithms. Securing the foundation of our digital infrastructure becomes paramount, requiring the development and implementation of quantum-resistant protocols *(Dr. Vincent, 2022).*

Standards and Regulations: A Collaborative Endeavor

Addressing the security challenges posed by quantum computing requires a collaborative effort between researchers, industry experts, governments, and the policymakers. The establishment of quantum-safe standards and regulations is crucial to ensure a seamless transition to a post-quantum security landscape. International organizations such as the National Institute of Standards and Technology (NIST) are actively involved in the standardization of post-quantum cryptographic algorithms. Their efforts aim to foster interoperability, promote secure practices, and provide guidelines for the implementation of quantum-safe solutions *(Quehen, 2022).*

Conclusion

The emergence of quantum computing presents a paradoxical reality where extraordinary computational power coexists with formidable security challenges. By recognizing and addressing the vulnerabilities through post-quantum cryptography, quantum key distribution, infrastructure protection, and the establishment of quantum-safe standards, we can navigate the quantum paradox.

References

Crane, 2022; A Look at Quantum Resistant Encryption & Why It's Critical to Future Cybersecurity; Available at https://www.thesslstore.com/blog/quantum-resistant-encryption-why-its-critical-to-future-cybersecurity/. [Accessed on 03 July 2023]

Dr. Rijmenam, 2023; Encryption and Quantum Computing – Fighting the Big Crunch of 2025; Available at https://www.thedigitalspeaker.com/encryption-quantum-computing-fighting-big-crunch-2025/. [Accessed on 03 July 2023]

Dr. Vincent, 2022; The Quantum Threat to PKI - Infrastructure for Financial Services. Available at https://arqit-res.cloudinary.com/image/upload/v1643293689/WhitePapers/The_Quantum_Threat_to_PKI_Infrastructure_for_Financial_Services_ctn7ao.pdf. [Accessed on 03 July 2023]

Finance Magnates, 2023; Harnessing Quantum Computing for Financial Analysis and Risk Management. Available at https://www.financemagnates.com/fintech/data/harnessing-quantum-computing-for-financial-analysis-and-risk-management/ [Accessed on 03 July 2023]

Farckiewicz, 2023; Quantum Computing and AI: A Powerful Partnership for Scientific Discovery. Available at https://ts2.space/en/quantum-computing-and-ai-a-powerful-partnership-for-scientific-discovery/. [Accessed on 03 July 2023]

Herman, Googin, Liu, Galda, Safro, Sun, Pistoia, Alexeev, 2022; A Survey of Quantum Computing for Finance. Available at https://arxiv.org/pdf/2201.02773.pdf [Accessed on 03 July 2023]

Infinity Foundation, 2021; Quantum Computing & National Security - TIFR Scientist. Available at https://www.youtube.com/watch?v=Cd6nFzh_70Y [Accessed on 03 July 2023]

Institute of Medicine of the National Academies, 2014; Improving and Accelerating Therapeutic Development for Nervous System Disorders: Workshop Summary. Available at https://www.ncbi.nlm.nih.gov/books/NBK195047/ [Accessed on 03 July 2023]

National Security Agency, 2023; Quantum Key Distribution (QKD) and Quantum Cryptography (QC); Available at https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. [Accessed on 03 July 2023]

Newton W, 2023; Quantum medicine: how quantum computers could change drug development. Available at https://www.clinicaltrialsarena.com/features/quantum-computers-drug-development/ [Accessed on 03 July 2023]

Nohe, 2018; Let's talk about Post-Quantum Encryption. Available at https://www.thesslstore.com/blog/post-quantum-encryption/ [Accessed on 03 July 2023]

Patel,R (2023); Maximize Your Logistics Efficiency with Supply Chain Route Optimization Handbook. Available at https://www.upperinc.com/blog/supply-chain-route-optimization/ [Accessed on 03 July 2023]

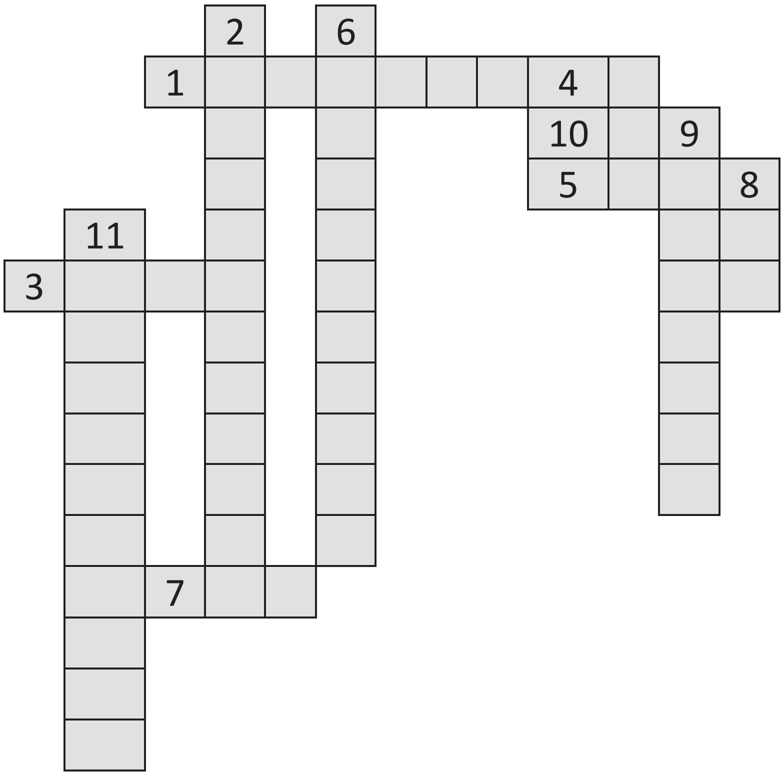
Quehen, 2022; NIST Announces their Post-Quantum Cryptographic Algorithms for Standardization. Available at https://www.infosecglobal.com/posts/nist-cryptographic-algorithms-for-standardization. [Accessed on 3 July 2023]

Weinberg S, Sanches F, Ide T, Kamiya K, Correll R, 2023; Supply chain logistics with quantum and classical annealing algorithms. Available at <https://www.nature.com/articles/s41598-023-31765-8> [Accessed on 3 July 2023]

ANSWER FOR Q2 2023 CROSSWORD

				N												
			W	O	R	K	F	A	C	T	O	R				
				N					E	L						
				R				H	A	S	H	I	N	G		
				E					S							
				P	G	P			A							
			Q	U	B	I	T	S	R	I	J	N	D	A	E	L
	D			D								O				
D	I	F	F	I	E	H	E	L	L	M	A	N				
	F			A		S						E				
	F			T		M										
	U			I												
	S			O												
	I			N												
	O															
	N															

ISACA BANGALORE CHAPTER CROSSWORD PUZZLE (Q3 2023)



ACROSS	DOWN
1. Nothing inside the organization is automatically trusted. (9) 3. Security Model with focus on Integrity. (4) 5. Anything as a service. (4) 7. This is a solution that restricts access to privileged accounts or detects when accounts use any elevated privileges. (3) 10. Attack on computer network to prevent a system from responding to legitimate request for service. (3)	2. Security Model with focus on confidentiality. (12) 4. Refers to a trend of replacing hardware with software. (3) 6. This is one of the controls to check insider frauds: (11) 8. A document that Stipulate performance expectations and often include penalties if the vendor doesn't meet expectations. (3) 9. Process of removing data while a hardware is being disposed. (8) 11. This attack employs over-sized ping packet. (11)

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 **November 25th, 2023.**

Annual Karnataka Conference

ISACA Bangalore Chapter

ISACA Bangalore Chapter

DAY 1

2023 - ISACA - BC - Annual Conference - Date - 28th July 2023
The LaLiT Ashok Bangalore

Time	
08:30 - 09:30	Registration
09:30 - 09:45	Welcoming the Chief Guest & Keynote speaker to the venue
09:45 - 09:55	**Welcome** by Conference Chair - ISACA BC Vice President Ms. Vijaya Vanitha
09:55 - 10:00	Chief Guest, Keynote speaker & ISACA office bearers ascend the dias Dr. M.A. SALEEM, IPS Director General of Police, Criminal Investigation Department, Special Units and Economic Offences. Mr. Mahadesha / Program Director & Ciso, CeG - Government of Karnataka
10:00- 10:10	**Inauguration - Lighting the lamp**
10:10 - 10:20	Welcome by ISACA BC - President Rajasekharan KR
10:20 - 10:40	Inauguration address by Chief Guest Shri. Dr. M.A. SALEEM, IPS
10:40 - 11:00	Keynote address
11:00 - 11:10	Release the conference edition of newsletter by Chief Guest
11:10 - 11:25	Felicitation by Chief Guest (High exam scorers)
11:25 - 11:45	**Exhibits & Tea Break**
11:45 - 12:20	**Session 1 - Do More with Less: Navigating Top Cyber Risks and Regulatory Requirements** Mr. Prateek Bhajanka - APJ Field CISO - Sentinelone
12:25 - 13:00	**Session 2 - The Future of Cyber Security is Here** Ms. Jyothsna Chalasani -Demand and Delivery Manager- Optiv Karthik Sridharan, Senior Consultant – Optiv Security Inc
13:00 - 14:00	**Lunch Break**
14:00 - 14:30	**Session 3 - The India DPDP(Data Privacy Bill) and the Security Legislative Landscape** Mr. Sajai Singh JSLaw - Partner
14:30 - 15:00	**Session 4 - Digital Immunity: Cultivating Resilience in the Face of Cyber Threats** Mr. Krishnadev A - Head - Presales & Senior Cybersecurity Solutions Architect - Innspark
15:00 - 15:30	**Session 5 - Web Security: Emerging Threats and a Smart Platform for Defence** Mr. Vaisakh Rajeevan - Founder and Chief Architect of Prophaze
15.30 - 15.45	**Exhibits & Tea Break**
15.45 - 16:40	**Session 6 - Panel Discussion** **The digital transformation era: cybersecurity, AI and Machine Learning demystified** Moderator - Mr. Shanker Sareen - Head - Marketing, India & Saarc Ms. Uma Rani T M - SVP and Head of Private Cloud Products - SAP Mr. Lokesh Gowda - Optiv - Vice President and General Manager Ms Sarada Vempati, EVP, Head of Enterprise Functions Technology, India & Philippines Wells Fargo
16:40 - 17:15	**Session 7 - AI resurfacing the Landscape of Privacy** Ms. Sindhu Shaji Vethody - Senior Director - Protiviti
17:15 – 17:25	**Winners of Quiz**
17:25 – 17:30	**Vote of Thanks**

26

Annual Karnataka Conference

ISACA Bangalore Chapter

ISACA

Bangalore Chapter

DAY 2

2023 - ISACA - BC - Annual Conference - Date - 29th July 2023
The LaLiT Ashok Bangalore

Time	
09:00 - 09.05	Welcome by ISACA Bangalore Chapter - President Chief Guest & ISACA office bearers ascend the dias
09:05 – 09:45	Chief Guest & Keynote speech B Dayananda IPS **-** Police Commissioner - Bengaluru City J A Chowdary - Entrepreneur, Innovator, Angel Investor, An Industry Leader
09:45 - 10:15	**Session 1 - Navigating AI : Digital transformation, Balancing Progress and Social Responsibility** GIRIDHAR JAKKI - Senior Director - Samsung Research India
10:15 - 10:45	**Session 2 - The Critical Need for a Common Fintech Framework** Mr. Pratyush Kukreja - Business Head, APAC, Scrut Automation
10:45 - 11:15	**Session 3 - Does the "metaverse" approach a tipping point?** Mr. Venu Ganapuram - Principal Scientist - CSIR
11:15 - 11:30	**Exhibits & Tea Break**
11:30 - 12:00	**Session 4 - Securing the AI – New Battle front for Defenders** Mr. Manoj Kumar Parmar - Founder - CEO, CTO - AIShield
12:00 - 12:30	**Session 5 - The Ascendence of AI in Human Resources: Unveiling the Converging Pathways With Cybersecurity** _ Mr. Vishwanadh Raju **-** Head - Talent Acquisition - ANSR
12:30 - 13:00	**Session 6 - Data Clean Rooms in the Age of Digitization: Hype or Reality?** Gowthaman Ragothaman - Founder - Aqiliz -Singapore
13:00 - 14:00	**Lunch Break**
14 : 00 - 14:15	Quiz by ISACA BC : Survey opportunities for Sponsors
14 :15 - 14:45	**Session 7 - Managing Perspectives for Assessment Reports with Few or Zero Findings** Mayank Pal Singh - Practice Manager, Application Security - Optiv
14:45 – 15:15	**Session 8 - Cyber Warfare & Digital Battlefield - Are we ready ?** Mr. Robin Philip Varghese - Global Head - Platforms, Engineering and Applied Intelligence DXC Technology
15:15 - 15:30	**Exhibits & Tea Break**
15:30 – 16:20	**Session 9 - Panel Discussion** **The C - Suite Debate - Next-generation Privacy Promoting Global Data Governance System Interoperability To Permit International Data Flows** Mr. Sandeep Rao - Chief Product Officer - Arrka (Moderator) Mr. Gowthaman Ragothaman Mr. Rajesh Viswanathan, Senior Group Manager - Infosys Ms. Shefali Sonpar - Insurance Expert, Digital Transformation Evangelist
16:25 – 16:55	**Session 10 - Building Successful Privacy Program** - **Compliance Based to Privacy Engineering** Amit Kaushik - Data Protection Officer - Zee Entertainment Enterprise
17:00 – 17:10	Winners of Quiz, Social Media & Sponsers Booth Passport Lucky Draw
17:10 – 17:20	**Valedictory Address** Mr. Raghu.R.V - ISACA Regional Ambassador
17:20 – 17:30	**Vote of Thanks**

26th Annual Conference held on 28th & 29th July 2023

A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats

26th Annual Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
28th & 29th July 2023
The Lalit Ashok - Bangalore
A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats
SPONSOR

26th Annual Conference held on 28th & 29th July 2023

A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats
ISACA

26th Annual Karnataka Conference
ISACA Bangalore Chapter
ISACA
Bangalore Chapter
28th & 29th July 2023
The Lalit Ashok - Bangalore
A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats

SmartTech Asia 2023 Conference held on 14th September 2023

Inauguration of SmartTech Asia at ISACA

Report on the ISACA SmartTech 2023 Conference themed

"Secure Your Digital Interactions and Transactions: The Modern-Day Imperative of Digital Trust"

Community Day held on 7th October 2023

ISACA celebrated Community Day on Saturday the 7th October 2023. As part of ISACA Bangalore Chapter Community day, volunteers from our Chapter visited the NGO Sparsha (Makkala Dhama) located on outskirts of Bangalore City. Community Day exemplifies our purpose, promise and values with a day of service around the world. Not only we can help individuals realize the positive potential of technology, but together, we can help people realize the positive potential of ISACA's global network.

Move Your Career Forward with ISACA Certification
Get certified and get ahead.
CISA
CISM
CRISC
CGEIT
CDPSE
CSX-P
www.isaca.org
ISACA
Bangalore Chapter

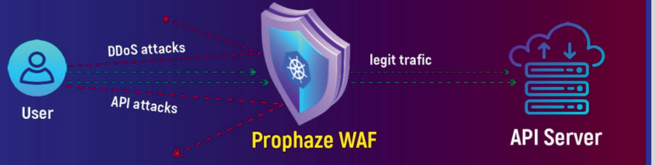
Cybersecurity Awareness Session at SRLDC, Grid India for CISO and Team held on 19th October 2023 at their Campus

In view of the observance of Vigilance Awareness and Cyber Security Awareness Month; ISACA BC conducted an awareness session on Cyber Security and Cyber Hygiene at SRLDC on October 19, 2023. CISO SRLDC and all the employees attended from GRID-INDIA (SRLDC).

Prophaze

The New Phase of Security

How Prophaze works?



World's first pure Kubernetes driven Web security Platform

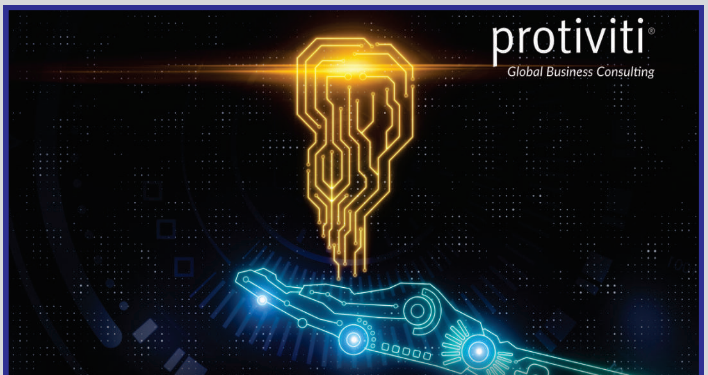
Cloud Native | AI / ML Based threat profiling
Multi cloud deployments | Virtual Patching
Low false Positives | Fast and easy onboarding

100% Protection From all web attacks

E-mail: security@prophaze.com | www.prophaze.com
Contact : US (+831) 217-6365 IND : +91 79940 08420

protiviti

Global Business Consulting



EMBRACING OPPORTUNITIES THROUGH **EMERGING TECHNOLOGIES**

We help companies make the promise of digital transformation a reality.

- Internal Audit
- Data Analytics
- Technology Consulting
- Cyber Security Services
- Business Operations Improvement
- Governance, Risk & Compliance
- Forensic Services
- Financial Risk Management
- Strategy & Transformation
- Human Capital Consulting
- Transaction Services
- Digital Transformation

Our India offices:

Bengaluru Phone: +91.80.6780.9300	**Delhi NCR** Phone: +91.124.661.8600	**Kolkata** Phone: +91.33.6657.1501
Chennai Phone: +91.44.6131.5151	**Hyderabad** Phone: +91.40.6658.8700	**Mumbai** Phone: +91.22.6626.3333

India@protivitiglobal.in

www.protiviti.in

સ | Sameeksha

Sarvaiya Infotech

Audit Management Software

One Organisation. One Audit Software.
Build your own audit workspace.

- **One Organisation**
- **One Software**
- **Multiple Departments**
- **Multiple Audit Types**
- **Multiple Audit Templates**

End to End Tool

- Create your task databank.
- Plan your assignment.
- Assign Resources to Audits.
- Assign Tasks to Audits.
- Work on Web and mobile.
- Assignment based review workflow.
- Track the assignments.
- Upload your working paper
- Download report.
- Follow up.

+91 86187 01018

92A, 2nd Main, GoodWorks Infinity
Park, Electronic City Phase 1, Bengaluru - 560 100

namaste@sarvinfo.com
www.sarvinfo.com

Scrut Automation

Are you tired of going through multiple **audits with overlapping requirements?**

REGUSENSE
has got you covered!

With 25+ frameworks combined into **ONE comprehensive framework,** RegUSense will save you 100+ hours by achieving **compliance with overlapping requirements in ONE GO!**

Scan here for a CONSULTATION

Hackers work hard.
We work smart.
sentinelone.com

innspark
Explore.
Transform.
Fortify.

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