ISACA
Bangalore Chapter

Q2 - 2023 ISSUE

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

26 Annual Karnataka Conference

ISACA Bangalore Chapter

28th & 29th July 2023
The Lalit Ashok - Bangalore

THEME : A HERMIT OUT OF ITS SHELL : DIGITIZATION, PRIVACY, CYBERSECURITY AND 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

ISACA Bangalore Chapter

InfocITy Auditor

Q2 - 2023

From The Desk Of The President

We hope this message finds you healthy and happy.

I would like to thank all of you for your active support and participation.

We are pleased to announce the launch of our brand-new website! The new site is now available at www.isacabangalore.org. Our current website, hosted on the ISACA Engage site, will continue to be updated and can be accessed at https://engage.isaca.org/bangalorechapter/home. Hope to see more engagement on the new website. More features and updates will be included in the upcoming weeks and months.

I hope you have noticed the 50th anniversary of ISACA Journal and its trajectory; indeed, it is an amazing gift to the community and a dedicated effort by our volunteers. In the next 50 years, I am sure ISACA will deliver high-quality content across a wide spectrum of media, including blogs, vlogs, podcasts, and ebooks, for our members.

Recently, ISACA announced **free membership for the year 2023** to the students, and this is the first ever announcement of its kind considering India's growth story in the information technology and security domains. Following the announcement, we have approached various universities and colleges. We have sent the membership invitation to five universities and 500+ students based on the confirmation. I hope to see more student members in the ISACA Bangalore Chapter.

EC members also visited BMSIT Yelahanka, Garden City College, and Jain University JC Road to promote the free membership drive.

ISACA Bangalore Chapter participated in a national-level seminar on Cybersecurity at the prestigious Information Warfare School in Air Force Station Jalahalli on July 10–11. The theme of the seminar is "Information Assurance in the Age of Net Centricity." The seminar is inaugurated by the Air Marshal and other senior officers of the Air Force. Eminent speakers from NSC, NCSC, DCyA, UIDAI, CIRA, MeitY, and other organizations participated. I have had the privilege to represent ISACA and share the guest session on Enterprise Security and Risk Management: Best Practices. We hope going forward ISACA Bangalore chapter will be able to partner with IAF on various cybersecurity initiatives and trainings.

Registration has started for the 26th Annual Karnataka Conference of ISACA Bangalore, which is the largest in-person gathering of the year for our chapter. The Annual Karnataka Conference 2023 will bring together leaders and cybersecurity professionals committed to turning ideas into reality. We believe that you will learn how to build a stronger network, enhance your business acumen, and advance in your profession.

The 26th Annual Karnataka Conference, on the theme **"A Hermit out of its Shell: Digitization, Privacy, Cybersecurity, and Current Threats," will be held at The LaLit Ashok, Bengaluru.**

A full day of **complementary** training on **"Building a Privacy Program"is** planned as an early bird discount for early bird option registrants. We have seen an incredible response for our 26th Annual conference. Before one month of registration, we had more than 200 registrations, and it is the first time in the history of the ISACA Bangalore chapter that we achieved such a number well before the event.

We strongly believe that our members deserve recognition for their affiliation with our chapter, and positivity is now more important than ever. Let's join our 26th Annual Karnataka Conference and make it a memorable one.

Lastly, before I sign off, I would like to say a huge thank you to our chapter EC and members for all their hard work throughout the last few months, and my best wishes to all for our 26th Annual Karnataka Conference of ISACA Bangalore. I am sure we are moving steadily towards one of the largest annual conference gatherings by the ISACA Bangalore chapter. I hope to see a positive transformation in all activities of our chapter, which will help transition into a brighter future.

Regards

RAJASEKHARAN K R, CISM, CDPSE, CRISC, PMP, ITIL (E), CSM, SAFe, ISO 27001 LA

Message From the Vice President

Dear Members,

I sincerely hope this message finds each one of you in good health and spirits!

As India's largest Chapter, ISACA Bangalore Chapter, our Board and Volunteers remain dedicated to providing you, our members and the rest of the world with innovative learning content, programs, membership outreach and events.

By now many of you should be aware that our 26th Annual Karnataka Conference 2023 themed "A Hermit out of its Shell: The Digitization, Privacy, Cybersecurity & Current Threats" is happening next month on 28th & 29th July, 2023 at The LaLit Ashok Hotel, Bengaluru.

The Board of Directors and I are excited about the opportunity to see you in person! We value your patience as we have been preparing and working in the background to give you a fantastic experience!

We have a great line-up of experts, who will share their insights on the trends they are seeing in Digitization, Privacy, Cybersecurity & Current Threats and Technology's impact on the careers of professionals and the organizations they belong to.

So, what are you waiting for? Go-ahead, register and learn more about our speakers and panellists!

We hope to see you there!

I along with the ISACA Bangalore Chapter Board thank our sponsors, partners and alliances for their continued support and participation in our chapter events. Your contributions and efforts are much appreciated!

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

Message From Secretary

Dear Members,

I extend a very warm greeting to all of you. This is our special edition of the newsletter being released during the 26th Annual Conference on the 28-29 July 2023.

We have arranged a galaxy of speakers on cybersecurity and also we are supported by a number of sponsors for the programme. Various Top Government Officials have committed to attend the program. It will be an exciting event, request you not to miss the same. It will be a good networking and a knowledge enhancing opportunity.

We are proud to inform you that we continue to remain the largest chapter in India, thanks to all our members for the same. We request all our members who are yet to renew their subscriptions to renew membership and enjoy all the membership privileges extended by ISACA. This will enable you to grow in your career and get recognition in the community as leaders in the IT space. The certifications offered by ISACA continue to remain among the top certifications in the recently conducted surveys across the Globe in the IT industry. The certified CISM and CRISC holders are most sought after by the Employers offering good remunerations.

We are in the process of launching our chapter's new website as decided during the previous AGM. The website is prepared and is under final stages of testing and will be launched shortly, probably before the Annual Conference. It will be displaying the activities being conducted by the chapter. The URL will be shared once the websites goes live.

Once again, we request you to please register for the conference and utilise the opportunity to network during the conference and grow your knowledge, with all the thought leaders putting across their insights on Cybersecurity.

Adios, would be glad to meet you in all in person during the annual conference.

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.

Those who have not renewed their membership, now it is time to reinstate your ISACA® membership for 2023. If you have not already done so, it is not too late to reinstate your membership. Please ensure to reinstate your membership before the final removal of your name from the member list to ensure the benefits arising out of continued membership.

Please click below to renew/reinstate *(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 2023 membership renewal: **US$ 145.00**

ISACA also offering a Half Year/Half Price Dues for New Members

During the months of June and July, ISACA will offer a "half year/half price" dues promotion, when ISACA Global dues for individuals who join are reduced by half to: Please keep a watch on this on ISACA website.

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://tinyurl.com/4m4fex9k

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

CISA Certified Information Systems Auditor	CISM Certified Information Security Manager	CRISC Certified in Risk & Information Systems Control	CDPSE Certified Data Privacy Solutions Engineer	CGEIT Certified in the Governanceof Enterprise IT
5 Weekends	4 Weekends	4 Weekends	3 Weekends	4 Weekends
Domain 1 19-Aug Information Systems (IS) Auditing Process	Domain 1 05-Aug Information Security (IS) Governance	Domain 1 09-Sep Governance	Domain 1 15-Jul Privacy governance	Domain 1 23-Sep Governance of enterprise IT
Domain 2 20-Aug Governance and management of IT	Domain 2 06-Aug Information Risk Management	Domain 2 10-Sep IT risk assessment	Domain 2 16-Jul Privacy architecture	Domain 2 24-Sep IT resources
Domain 3 26-Aug IS Acquisition, Development, and Implementation	Domain 3 12-Aug IS Program Development and Management	Domain 3 16-Sep Risk response and reporting	Domain 3 22-Jul Data lifecycle	Domain 3 30-Sep Benefits realization
Domain 4 27-Aug Information systems operation and business resilience	Domain 4 13-Aug IS Incident Management	Domain 4 17-Sep Information technology and security		Domain 4 01-Oct Risk optimization
Domain 5 02-Sep 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
98805 29503
96634 00039

ISACA
Bangalore Chapter

Annual Karnataka Conference

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

28-29 Jul 2023

The LaLiT Ashok

20+ Speakers and sessions

Sponsors

Prophaze · innspark · OPTIV · protiviti · SentinelOne · Sarvaiya Infotech · Scrut Automation

To Register Scan the QR or go to link https://tinyurl.com/4fx8334n

Recap of Chapter Programs in Q2, 2023

CPE Sessions:

1. **Topic : "Re-Imagine : Shift Left Security"**
   Speaker : Mr. Amit Butall, Vice President at Wells Fargo
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 22-Apr-2023 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Free Attendance : 2 CPE Credits offered

Topic Summary:

Reducing Risk across Software development life cycle requires a collaborative, multi-disciplinary framework to embed security into SDLC holistically within the hyper agile speed of DevOps and shifting security left

Speaker Profile:

Amit is a cybersecurity and risk management leader with over 19 years of progressive experience. During the course of his experience, he led and acquitted many skills and exhibited them in delivering various transformations in customer centricity, information and cyber security, technology risk and control assessment, IT audits and compliance, control design, data governance, and agile delivery across business groups by providing strategic direction, a future road map, IT governance, coaching, and stakeholder alignment.

Amit has the ability to adapt and learn quickly in challenging and changing environments through the knowledge assimilated through professional experience and certifications in CRISC, CISA, CISM, CGEIT, DevSecOps Practitioner, Professional Agile Coaching, and SAFe SPC Certified.

2. **Topic : "Managing the Attack Surface"**
   Speaker : Sangamesh S., Head - Cyber Defense Center
   Venue : Web-based ONLINE session via Zoom Webinar Platform
   Date : 20-May-2023 (Saturday) Time : 5:30 PM - 7:30 PM IST
   Free Attendance : 2 CPE Credits offered

Topic Summary:

In this ever-evolving digital world, organizations are expanding their business on Cyber. Having the prime objective of application purpose and functionality, at times, Security is considered after-math. This introduces vulnerability to the organization and creating an opportunity for the attacker for intrusion. The session will focus on an outlined agenda focusing mainly on identifying such an attack surface and how to manage it to reduce the cyber risk of the organisation.

1. Understanding Security Posture and Attack Surface Management
2. What constitutes the attack surface
3. How to recon
4. Developing remediation plan

Speaker Profile:

Sangamesh is an experienced and accomplished Information Security Professional with 18+ years of experience, spanning all facets of Information Technology and Security. His proficiency includes design & implementation of Enterprise security platform management, Security Operations, Incident response/management, Cyber Threat Intelligence, Counter Intelligence, Threat Research, Digital forensics, Vulnerability Assessment, Penetration Testing and Red/Purple Teaming. Sangamesh is working with Infosys. In his current role, Sangamesh is the Head of Cyber DefenseCenter. He is passionate about analyzing Cyber Threats and spends time on Cyber Threat Research. He spends his time orchestrating cyber-attack and understands the security controls effectiveness for detection / prevention. He is a frequent speaker in Cyber Security forums like Data Security Council of India (DSCI) and part of few Special Interest Groups (SIG) on Cyber Security research. He is also part of the WorldSkills team, representing India as an Expert for Cyber Security track. Under his mentorship, India has received the "Medallion for Excellence" in World Skills Kazan 2019 (Skill Olympics) and has received "Kaushal Acharya" award from the Ministry of Skill Development and Entrepreneurship of India.

3. Topic : "Design Shield : Leveraging Thread Modelling for Security Resilience"
Speaker : Mr. Mahesh Thimmaiah, Product Security Manager at Zeta
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 27-May-2023 (Saturday) Time : 5:30 PM - 7:30 PM IST
Free Attendance : 2 CPE Credits offered

Topic Summary:

Agenda:

Understand threat modelling techniques to identify security risks and vulnerabilities.

In this session Mr. Mahesh will delve into the core concepts of threat thread modeling and its critical role in proactive security strategies. This session will also highlight the practical implementation of threat modelling within organizations, with real-world examples. A Case study highlighting the successful application

Learning Objectives:

1) How to perform threat modelling

2) Different tools/techniques to perform threat modelling

3) How organisations with the above can ensure that their systems are secure and their users are protected.

Speaker Profile:

Mr. Mahesh Thimmaiah has 13+ years of experience in the VA/PT of web, mobile, and network systems, among other security engineering roles like security architecture, SSDLC, cloud security, etc.

Mr. Mahesh is OSCP & CDP certified and has experience in training developers and QA engineers in various organisations and in public forums like NULL.

Currently, Mr. Mahesh is part of Zeta working as a product security manager.

ISACA
Bangalore Chapter

Dear Members,

Please see the following information and offerings, including **many free CPE opportunities**:

CYBERSECURITY : NEW COURSES

- Advance your career with ISACA's essential, online cybersecurity courses. ISACA is now offering four hands-on, interactive cybersecurity courses you can take on your own time: Digital Forensics, Penetration Testing, Threat Hunting and Vulnerability, Identification & Analysis. Sign up today to earn up to 12 CPEs.

AWARDS

- **Nominate for ISACA Awards -** ISACA recognizes excellence in advancing digital trust though its prestigious awards program, which includes Global Achievement Awards, Hall of Fame, Chapter Awards, and Certification Exam Top Score Awards. Nominations for awards are open **until 15 August**. Nominate today! View the webinar to learn more. One hour/one **FREE CPE** credit.

DIGITAL TRUST

- **Volunteer** at ISACA Europe Conference 2023: Digital Trust World **and Save on Registration -** Volunteers are needed to support conference operations at ISACA's Digital Trust World conference in Dublin, Ireland, **17-19 October 2023**. Conference volunteers receive a 60% discount off the regular rate of registration. Sign up to volunteer now.
- **Podcast: Digital Trust Priorities for Privacy and Emerging Tech -** ISACA Digital Trust Advisory Council Members Anne Toth and Michelle Finneran Dennedy discuss privacy concerns and priorities around emerging tech and critical considerations for ensuring strong digital trust. Listen here.

ASK ME ANYTHING SERIES

- **"I'm an Artificial 'Intelligence' and ML Expert, Author, TED Speaker, and Teenager," Ask Me Anything! -** Join the online discussion **17-21 July** 2023 with Tanmay Bakshi, an accomplished tech prodigy, bestselling author, Google developer for machine learning, AI and software architect for IBM Watson Applications, professor, and TED speaker.
- **Subscribe** to the Emerging Technology community digest to stay up to date on the latest conversations, including this AMA!

RISK

- **FREE! ISACA Virtual Summit 2023: Risk Techniques to Build & Maintain Digital Trust - 19 July 2023, 9:00 am (CT) / 14:00 (UTC).** Due to rapid digital transformation, there must be a greater emphasis on risk management to protect the company's assets and brand. This summit will focus on risk management techniques to create digital trust among an enterprise's stakeholders and customers. Register here. Four hours/**FOUR FREE CPE**.

PROFESSIONAL DEVELOPMENT: MEMBER-EXCLUSIVE SPEAKER SERIES

- **The 3 Keys to Engaging People - 25 July 2023, 11:00 am (CT) / 17:00 (UTC) -** Scott Gould, an author and consultant on engagement, will share keys to successfully engaging people both internally and externally, and the psychological underpinning and operational application of engagement. Register here. One hour/one free CPE.

PRIVACY

- **Webinar :** Join the panel discussion webinar, "When Security Meets Privacy," in the Oceania time zone: **1 August 2023, 11:00 AM (UTC+10) Sydney**; which is **31 July** 2023 8:00 PM (CT). Find the day/time where you are here. An expert panel will discuss the need for an effective privacy and security program, where they intersect, and steps to implement them. Register here. One hour/one **FREE CPE** credit.
- **Free tool** for members: Privacy Regulatory Lookup Tool
- **Webinar: Data protection - It's all about people! - 30 August 2023, 11:00 am (CT) / 16:00 (UTC).** Data protection is often associated with abstract legal requirements or deep technical concepts yet only lip service is paid to what data protection is really about – people! This webinar will look at data protection from 2 angles: the data and people. Register here. One hour/one free CPE. All ISACA webinars are listed here.

COMPLIANCE

- **Webinar: The State of Compliance in the Financial Services Industry - 3 August 2023, 11:00 am (CT) / 16:00 (UTC).** Almost 600 people were surveyed about the state of compliance in today's evolving cyber landscape. Join as A-LIGN VP of Customer Success, Patrick Sullivan, delves into the most impactful findings from the survey to learn more about the past, present, and future of compliance in the financial services industry. Register here**.** One hour/one free CPE. All ISACA webinars are listed here.

CYBERSECURITY

- **White Paper:** Blueprint for Ransomware Defense(a member-only offering)
- **Webinar: Google Cloud Sponsored Webinar - The Future of Cloud Threat Detection, Investigation & Response - 10 August 2023, 11:00 am (CT) / 16:00 (UTC).** Learn how threat detection, investigation, and response (TDIR) in the cloud differs from traditional on-premises approaches, best practices for end-to-end workflows, solution recommendations to consider and future impacts on security operations. Register here**.** One hour/one free CPE. All ISACA webinars are listed here.

Cybersecurity in Autonomous Vehicles

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

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

Photo Credit: Cubicle Telecom

Can you imagine the vehicle of the future… perhaps the one with no steering wheel, and no pedals for acceleration and brakes and the one where you are not driving the vehicle. The vehicle of future is a big computer on wheels with enough room for few people to sit. The occupants of the vehicle could sleep, take rest or take official meetings. Would it be safer? Would it make your day more productive? As you read through this article, you can assume that your grand kid will never need to own a drivers license as the future grandkids will not be driving any vehicle.

I am exploring the ramifications of autonomous driving in the IT infrastructure space, as this involves Interconnected Vehicles, Vehicle Automation, Internet of Things, Machine Learning, Big Data and Shared Economy. This opens the pandora box of increasing attack surfaces for the vehicles of future, and the possibilities that your next car can be hacked. Almost every automobile company has reported hacking/ cyber theft incident in the past 15 years. In 2015, one of the major reasons GM recalled 2.7 million Jeeps was when the hacker walked up to the vehicle on the road, lets himself inside the vehicle, takes control of the steering wheel, starts the vehicle, and drives away as the new owner of the Jeep. And the ordeal was recorded on camera.

Apart from major automobile companies (including General Motors, Ford, Tesla, Toyota), several other companies like Waymo, Cruise, TuSimple, and Aurora are already testing driverless technology on public roads in the U.S., with some companies expecting to be fully driverless as early as 2024. When Tesla became the largest automobile company with $980 billion market capitalization despite selling less than a million vehicles; as compared to Toyota the second biggest automobile company that sold 10 million vehicles and market capitalization of $200 billion; there was a barrage of bear traders across the world desiring to short the stock as the stock valuation and stock metrics compared to its automobile peers (including vehicle sales, market capitalization, profitability, dividends, production costs, etc.) were comparable with each other, but was miles apart from Tesla…… this is because Tesla should not be considered as an automobile company. It's a Big Data and Artificial Intelligence company. Every time, Tesla drives on the road, it uploads all the information that it has gathered per kilometre. Information including the road dimensions, sidewalk dimensions, number of intersections, number of lanes, number of pedestrians crossing at the time, speed breakers, the thickness of the tar (asphalt) on the road, demographics of other car owners, traffic, nearest health centre, charging stations, weather, natural lighting, streetlights, nearby cameras, cellular service in the area, other Tesla cars in the neighbourhood and the possibility of interconnecting with other Tesla cars. This gets better when the second Tesla car drives on the same stretch of road – just like any algorithm. And this is the bedrock of mapping for autonomous vehicle driving.

Today's car has more computing power than was on board Apollo 11 spaceship that went to the moon. The average car today has 40 different computers, and high-end cars have as many as 100, and they're accompanied by 100 different electronic sensors. And it's not just the hardware that's ballooned, but the software too. Apollo 11 had 145,000 lines of computer code, but cars today can have more than 100 million.

What are these computers doing? Referred to as ECU's – short for Electronic Control Units – they run most of the functions of your vehicle. The biggest coordinates all the aspects of a car's engine, including the fuel injection rate to the ignition, throttle, timing, emissions, and cooling. Others monitor the anti-lock brakes, traction control, stability control, air bags, the windshield wipers, headlamps, and air conditioning. Then there are those that run the navigation system, music system, mobile phones, digital dashboard displays and, more recently, the driver assist systems.

Cyber threats to Autonomous Vehicle

- § Ransomware - Generally affects the car manufacturers, Original Equipment Manufacturers (OEM), attacks on supply chain for Tier 1 and Tier 2 dealer networks and maintenance dealer networks. On an average, there is 10,000 suppliers for each vehicle. How easy could it be to have one of the suppliers with compromised IT security.

- § Engine Control Units - ttackers could use ECU's (including Engine ECM, Powertrain PCM, Suspension SCM, Vehicle Safety ECU to obtain access to the vehicle internal system.

- § Cloud Service Providers - Insurance services, driving records,
- § Denial of Service Attacks – Wheel Jamming, IoT endpoints on the wheels, brake systems
- § Remote Hacking – Wireless Carjacking, Key Fob cloning
- § Attack on IoT devices –GPS jamming, Bluetooth jamming, external sensors, entertainment devices

For many automobile and transportation companies, ransomware attacks have already happened. Upstream Security's report mentions a ransomware attack on the Australian transportation company Toll Group, which affected 1000 servers and 40,000 employees. And Honda was forced to stop production in June 2020 due to ransomware attacks on plants in Europe and Japan.

Given that new threats are constantly emerging, we have seen susceptibilities all the way along the supply chain. There has been some Intellectual Property theft from Industrial Research and Development groups, hacks into manufacturing operations, customer data theft and even the electrical charging networks are susceptible.

Andromeda Risk Consulting recommends three ways automakers can build secure vehicles. First, security must be part of the design of every component bringing all suppliers in one robust IT platform. Second, there needs to be a multi-layered cybersecurity solution that involves in-vehicle, IT network, and cloud security defenses. Third, automakers need to develop vehicle security operations centers to monitor, detect, and quickly respond to cyber incidents to protect vehicles, services, fleets, and road users.

Believing that any cyberattack will never happenis the easiest and least expensive path for any company. History has shown that attacks have happened to everyone.Doing threat modeling, assessment and audits are wise investments to mitigate attempts turning into realized threats to a business or life. Any hubris is false overconfidence.

References

https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=59b0e2917f65

https://www.caranddriver.com/news/a37453835/car-hacking-danger-is-likely-closer-than-you-think/

https://www.stealthlabs.com/blog/autonomous-car-security-adversarial-attacks-against-new-mobility/#:~:text=The%20apparent%20risks%2C%20such%20as,drivers%20and%20other%20road%20users.

https://ceinetwork.com/cei-blog/auto-computers-means-complicated-costly-longer-repairs/#:~:text=The%20average%20car%20has%2030,ballooned%2C%20but%20the%20software%20too.

https://cyberstartupobservatory.com/cyber-security-connected-autonomous-vehicles/

Resilience - The Need of the Hour

- Sabyasachi

About the Author:

Sabyasachi has 22 years of information security domain experience. He holds 25 international certifications, including CISSP-ISSAP, CISA, CISM, CRISC, CGEIT, CDPSE, CCSA, PMP, CCSP, CCSE, CEH, AWS SECURITY / ARCHITECT, CCNP, SABSA, etc. He has facilitated multiple book camps on CISSP, CISA, CISM, CRISC, and CGEIT. Currently, he is a chapter instructor and item writer for ISACA's CISA, CISM, CRISC, and CDPSE exams. Recently, he authored a certification book on CISSP and CCSP.

He is a Director (InfoSec) in a multi-national organization. His previous experience includes overall security governance, project management, client handling, stakeholder communications, IT audit & reviews, documentation & staff augmentation.

Abstract :

This whitepaper is about the BCP process and the highlighted steps. Also, the BCP audit and the future of BCP are also discussed. First, the BCP and DR activities should be considered recurring projects with an end date. At least the BCP activities should be performed annually or with significant strategic changes. Developing a BCP program should be viewed as a project, while maintaining it should be regarded as an operational activity. One of the key objectives is to analyze the current and future state of the Resiliency parameters inside an organization.

Two of my favorite superheroes are Spiderman and Batman. Do you know the primary keyword for their success and mantra of defeating villains? Yes, it is Resilience. The Oxford definition of Resilience is "**the capacity to recover quickly from difficulties; toughness."** No one can argue the importance of Resilience for an organization in the current dynamic world IT environment. The Business Continuity Process (BCP) and Disaster Recovery (DR) are primary tools.

Let's start this whitepaper with the essential steps of the BCP and DR. First, the BCP and DR activities should be considered recurring projects with an end date. At least the BCP activities should be performed annually or with significant strategic changes. Developing a BCP program should be viewed as a project, while maintaining it should be regarded as an operational activity.

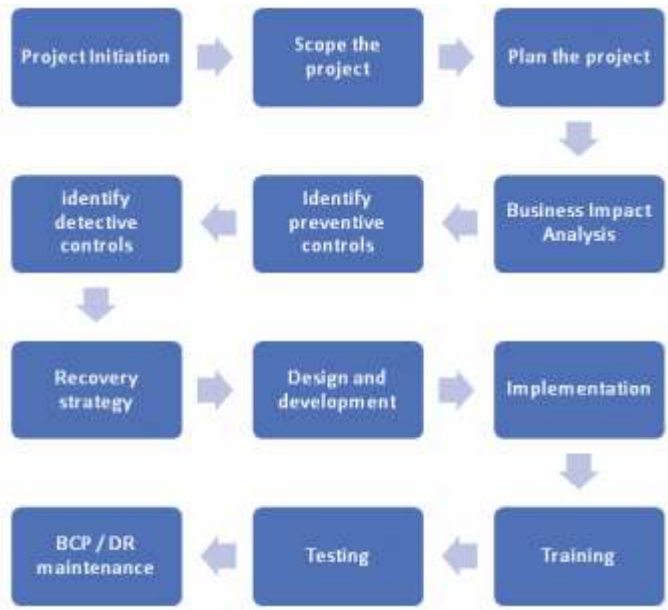
One of the key objectives is to analyze the current and future state of the Resiliency parameters inside an organization.

A few essential points to be considered while performing the gap analysis are listed below:

Developing a BCP/ DR is a complex process. However, a new BCP project is recommended if the current and future gap is enormous. Creating baselines and comparing with other similar organizations are also essential. Best practices in specific industries should be considered.

PROCESS FOR DEVELOPING A BCP/DR

This process is not only developing a new BCP program but also mapping the existing and required controls, which will enhance the overall resilience capability of an organization.



1. **Project Initiation**

   This phase identifies a need to create a new or edit the existing BCP program.

   The BCP project initiation typically include

   - Estimated budgeting and timeline
   - Required approvals
   - Define high-level scope
   - Determine the project sponsor and key stakeholders

2. **Scope**

   BCP program is done for an entire organization. However, the implementation and testing can be performed in phases depending on an organization's complexity and geographic distribution.

   The BCP project scope typically includes

   - Drafting a detailed scope
   - The business stakeholder should approve the scope
   - Regularity requirements should be part of the scope

3. **Plan the BCP project**

   Planning is always the most crucial part of any project. For planning, a BCP program should cover all the departments of an organization.

   The BCP project planning typically includes

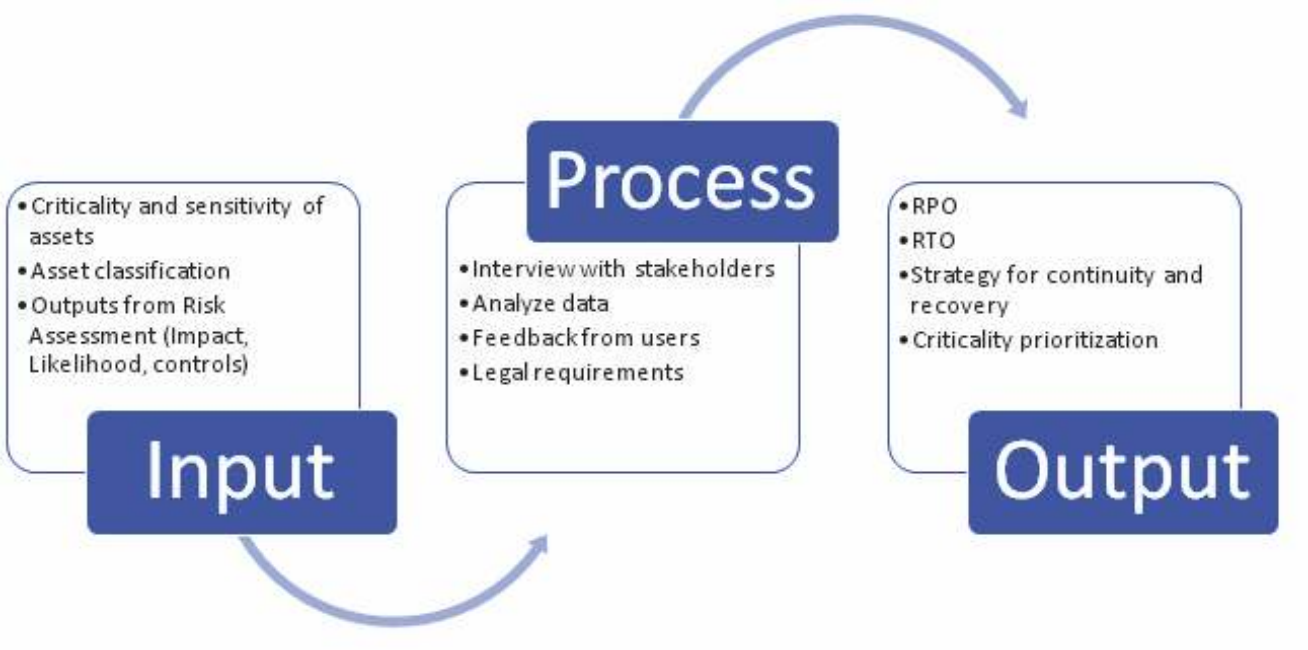
   - Risk plan
   - Policies and Procedures
   - Creation of Performance measurement baselines
   - Determine Roles and Responsibilities
   - Takeapproval of all plans and key deliverables
   - Cost
   - Schedule
   - Effort estimation
   - Vendor selection process
   - SLAs

4. **Business Impact Analysis (BIA)**

   Business Impact Analysis (BIA) is one of the most critical stages of BCP. This is a risk analysis about segregating the assets which require more attention. Therefore, setting up a priority is essential. For

example, if an organization's web server requires the minimum RTO and RPO, then the organization should invest more to ensure maximum uptime. Classification of data is one of the perquisites before the BIA.

The process of BIA is illustrated below



5. **Identify Preventive Controls**

Identifying the preventive controls are also essential. Preventive controls already in place in the organization ecosystem and how they can be mapped with the BCP program is a crucial exercise. Preventive controls are always preferred over detective controls. For example, automatic fire alarms.

6. **Identify Detective Controls**

Identifying the detective controls are also essential. The current detective controls list will help design the actual BCP program. For example, a fire alarm can be present in a data center. However, the process and monitoring of it may require fine-tuning.

7. **Recovery Strategy**

A few of the essential points to be considered in the Recovery strategy

- Select several critical applications and systems on a test basis to determine that appropriate backups are being executed
- Review the regulatory requirements
- Validate cost-benefit analysis
- On a test basis, the results of a critical process in the BCP test should be reviewed

8. Design and Development

The BCP deliverables should consist of

- Business risk and impact analysis
- Documented process to prepare the organization for various possible emergencies
- Detailed activities for dealing in the disaster event
- Procedure for managing business recovery processes
- Plans for basic training at multiple levels in the organization
- Procedures for maintaining BCP

A few of the essential points to be considered in the design and development are:

- Document the design of the overall BCP plan
- List out all the controls in detail
- Identify the task owner
- The design of the BCP program should always be based on the impact

9. Implementation

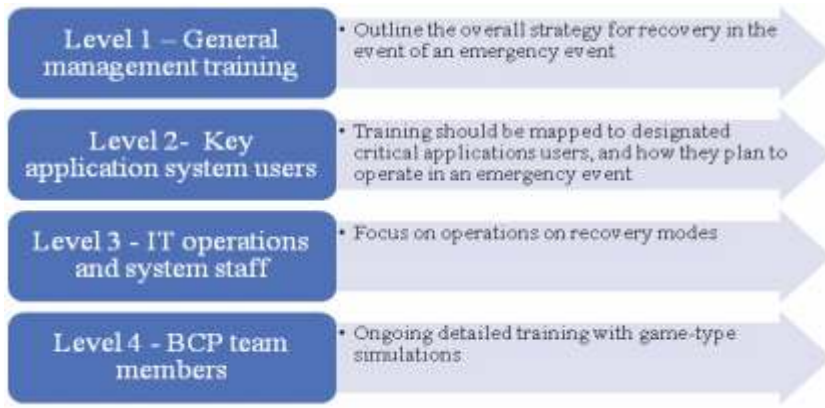
In this phase, the actual implementation is performed. Such as the backup requirements.

A few of the essential points to be considered in the implementation are:

- Implement the required component and controls to sustain the operations
- Determine that disaster recovery teams have been assigned and aware of their responsibilities
- Assess whether communication had been established with all necessary vendors and key stakeholders
- Determine that former processes have been selected for defining a disaster event and initiating the BCP
- All the required implementation should be routed and approved by the Change Management board

10. Training

The BCP training can be imparted in multiple level approach:



A few of the essential points to be considered in training are:

- Training should be tailored to the audience
- Training should be interactive and practical
- Training evaluations should be performed
- Feedbacks are essential

11. Testing

Testing the BCP plan is absolutely essential. In addition to planning and documentation based on recovery from actual incidents, an organization should schedule plan testing activities each year. Testing may range from simple tabletop exercises to a complete interruption test based on the requirements and necessity.

A few of the essential points to be considered in the testing are:

- Define which testing model will be used
- Testing can be performed in phases
- Testing should not impact production
- Document the testing results
- Testing approvals should be in place

12. Maintenance

The maintenance of a BCP program is always a challenge for an organization. It requires consistent effort and monitoring. Moreover, the BCP program should be considered one of the primary functions of an organization.

A few of the essential points to be considered in the maintenance are:

- Assess the adequacy of processes in place to keep current given differing application and technology changes
- Determine the procedures are in place to keep documentation correct, including communication with key stakeholders
- The establishment of adequately processes is a critical component of an organization's internal control structure

BCP Audit

Whether a manager, leadership team, auditor, or risk practitioner, it is crucial to be aware of the loopholes and visibility of improvement areas.

- Review the result of past internal audits for BCP

- Review overall training and understanding of the BCP
- Review the results of the recent BCP test
- Review of BCP backup procedures
- Review BCP policies and procedures
- Review service level agreements for the third party
- Interview IT operations personal
- Take the feedback from users

Future of BCP

As long as the business exists, the BCP will exist as BCP is the other name for resiliency.

More processes probably will be mapped with BCP, such as AI.AI will be part of the BCP process, especially in the incident management response. More proactive and preventive controls will be mapped with the AI. AI will be best in quickly launching a required sequence of activities without human errors and intervention. This requires gradual improvement and maturity. AI can also help in the prediction of an adverse event.

In this whitepaper, we have tried to cover the high overview of the BCP process among the audit requirements. We also touched the predicting the future of BCP as well.

Enough of technical talk. Let me start my newly purchased Spiderman Masterworks Vol 10 for the ultimate resiliency test. Take care.

References

1. *ACE CISSP, Sabyasachi Hazra, 1st edition, White Falcon Publishing*
2. *https://www.techtarget.com/searchdisasterrecovery/feature/How-to-use-AI-for-business-continuity-and-disaster-recovery-planning*
3. *Resilience definition from Wikipedia*
4. *https://www.b2bsustainable.com/bia-business-impact-analysis-explained/*

Identifying and Preparing for Interruptions, Disruptions and Emergence

- ***Anantha Sayana***, CISA, CISM, CIA

About the Author:

Has experienced the evolution of IT since its early days in the 1980s. After conducting information systems audits for more than a decade across systems in banking, finance, manufacturing, supply chain and project management in a variety of IT infrastructure landscapes, Sayana moved to a leadership role in core IT. He managed the implementation and maintenance of many solutions, including enterprise resource planning (ERP), web portals and the related IT setups used to build and manage information security in different software and domain environments. He has led digital transformation, including the implementation of new digital technologies such as the Internet of Things, augmented reality, virtual reality, mobile applications, big data analytics, machine learning and artificial intelligence for various solutions in engineering, manufacturing and project management. Four decades of experience have given him tremendous insight into managing, securing and auditing IT systems. Sayana is now retired and is currently involved in mentoring and teaching activities. He has volunteered with ISACA® for many years, including as a founding coauthor of the IS Audit Basics column in the ISACA® Journal and as a past Journal article peer reviewer. He was one of the founders of the ISACA Mumbai (India) Chapter and served as its president. He has also been a member of the CISA Test Enhancement Committee. He has spoken at numerous conferences and written many articles. He can be reached at asayana@gmail.com.

A beacon from a lighthouse or a buoy in the sea alerts passing ships of the presence of rocks or other dangers and guides the ships to safe harbor. Acts of guiding and alerting are embedded in the philosophy of information systems (IS) auditors. Dangers can be hidden, and guidance is required to reach destinations and achieve goals.

Just as ships face dangers, organizations may face different hardships that hinder their progress toward achievement of organizational goals.

These hardships can broadly be categorized as interruptions, disruptions and emergence events. It is important for IS auditors to understand the nature of these interruptions, disruptions and emergence events to help their organizations mitigate their adverse impacts.

Figure 1 shows how interruptions, disruptions and emergence differ from each other with respect to various dimensions. Understanding these differences is crucial to being prepared.

INTERRUPTIONS

An organization's information systems are expected to be available and functioning optimally to enable all users, internal and external, to perform their necessary actions at all times. However, systems can become unavailable or can malfunction, causing inconvenience or damage depending on the nature of the interruption and the length of the outage.

Interruptions can be classified into six major categories:

1. Software malfunctions
2. Hardware failures
3. Network outages, congestion
4. Malware, cyberattacks
5. Natural disasters (e.g., floods, fires, earthquakes)
6. Infrastructure events (e.g., power supply or air conditioning issues, civil disturbances)

The potential for each of these types of interruptions is known and examples have already occurred; therefore, strategies, methods, processes and tools exist for mitigating or recovering from each of them.

A proactive, well-managed organization should be prepared for all categories of interruptions. Although interruptions can occur suddenly and without notice, a prepared organization is ready to quickly swing into action, mobilize its workforce and find a solution. Security and audit functions have built sound processes, technologies and methodologies to prepare for these interruptions and either to prevent them or recover from them swiftly.

FIGURE 1
Interruptions vs. Disruptions vs. Emergence

	Interruptions	Disruptions	Emergence
Timing of occurrence	Sudden; unannounced	Not sudden; initially slow then accelerating	Gradual; takes time to be noticed
Targets affected	Potentially any system	Sometimes localized to a sector or industry or geography, sometimes localized to a technology	Could be widespread
Time to react	Very short	Reasonable time, but requires a strategy and plan	Adequate time; requires vision and futuristic thinking
Time to impact	Immediate	Medium; several months to a year from the first signs of trends and early adapters	Long; enough time to prepare for those who can see it coming
Nature of impact	Minor to severe depending on the nature of the interruption	Gradual, but could be severe leading to a threat to survival	Slower and could lead to loss of business and reduced lifespan
Preparation and mitigation	Well-known strategies, processes, technologies exist Need for operational readiness and response	Requirements for awareness of trends and reading the indicators of change Need for forward-looking leadership and the will to embrace change and innovative	The ability to read signals in the environment and industry Need for long-term vision and strategy and considerable preparation that may require time, effort and resources
IS auditor role and influence	Significant; evaluation,. verification and audit	Moderate; alerting, guiding advisory	Minimal; possible to guide and influence if IS auditor can get a seat at the table

The IS auditor's role in dealing with interruptions is significant. The IS auditor should participate in the risk assessment to identify all possible interruptions and their impact on specific systems. The auditor should also review all the mitigating control measures put in place and verify that they all have been tested and will be operational at the time of need. In addition, the IS auditor should evaluate all recovery and business continuity plans to ensure that they will succeed in restoring systems when interruptions happen. This should be an ongoing

process since systems and environments constantly change and plans must be updated accordingly. It is also necessary for the IS auditor to examine the preparedness of people—including staffing adequacy, staff training and staff ability to respond with agility during crises.

DISRUPTIONS

A disruption is not merely an interruption that temporarily halts operations. A disruption could potentially strike at the root of the very existence of something. It often goes beyond the technology and information systems and impacts the organization itself. Disruptions do not happen suddenly, such as with a cyberattack. Rather, they develop over a period of time and eventually cause change.

Emerging Technology Disruptions

Disruptions are often caused by the advent of new technologies. For example, banking in the 1990s required a customer to physically visit a bank branch to perform any kind of transaction. However, with advancements in network technology, the increasing reach and reliability of the Internet, and the creation of mobile applications (apps), banking account has changed dramatically. With the advent of online banking, customers can log in to their bank account and complete any transaction digitally. Banks that kept pace with technology and enabled their systems for online banking were successful, while those that did not had to play catch-up to survive.

The digital revolution has made mobile phones and their applications the mainstay of most business interactions and transactions. The Internet of Things (IoT) enabled products other than computing devices to connect to networks. Cars, household appliances, machinery and lights can now be fitted with the appropriate sensors to interact with networks. Manufacturers that failed to see this development and did not ready their products with these features were left behind by organizations that adapted quickly.

Technology developments in the fields of artificial intelligence (AI), machine learning (ML), automation, blockchain and the metaverse have led many organizations to implement these emerging technologies into their solutions and products to stay competitive. But emerging technologies can also become disruptors. While AI is already emerging as a disruptor in many fields, it remains to be seen whether the metaverse will converge the digital world with the physical in new ways. Will cryptocurrencies rule the world economy? Will blockchain become a more pervasive platform for transactions? As the world becomes largely digital, and interactions and monetary assets are predominantly digital, how is digital trust established? The risk associated with these emerging technologies needs to be understood and evaluated by IS auditors proactively so that they are not taken by surprise when large-scale deployments happen.

Nontechnology Disruptions

There are also nontechnological disruptions. The most recent example is the global COVID-19 pandemic.

The virus confined people from all walks of life inside their homes and prevented social contact amid an atmosphere of fear, stress, sickness and loss of lives.

It was digital technologies that enabled work from home (WFH), but not all organizations had the necessary technology infrastructure and processes in place to enable it. However, over time, remote work has become an accepted reality and hybrid models have been developed. Enabling security in the new work environment created challenges and resulted in losses for many organizations. A disruption of plans in place.

Man-Made Disruptions

Man-made events, such as wars, also cause disruptions and are more difficult to handle. The war in Ukraine is one such example that has had an impact far beyond its geography, impacting the energy sources and supply chains of many countries and enterprises.

Disruptions do cause distress, but organizations that have a forward-looking vision, organizational strengths and operational agility to innovate and respond to change have overcome disruptions and emerged stronger.

The Role of the IS Auditor

The IS auditor's work with respect to disruptions can be contributory and advisory. When the disruption that is happening in the industry is visible but the organization is not putting in effort to prepare for the disruption, the IS auditor can leverage relationships with senior management and the board of directors (BoD) to bring the issue to their attention and request guidance in terms of recommended action. By preparing and training in the use of disruptive technologies using resources from industry leaders and educators, the IS auditor can effectively participate in designing appropriate controls to be built into these new solutions. Hence, learning, training and keeping pace with technology are key requirements for IS auditors to make effective contributions toward dealing with disruptions.

EMERGENCE AND GLOBAL TRENDS

Technologies and the business scenarios in which they are applied have evolved in a mostly gradual manner, albeit with periodic abrupt changes. Certain trends can be seen in their nascent form but take some time to mature, become powerful forces and make an impact. Often these forces become pervasive and make their impact across geographies, industry sectors and technologies.

Such trends can be termed as emergence, for when they are first noticed, they are considered emerging. At any point in time there may be many trends that are somewhat visible, but not all of them will mature to make a significant impact. Identifying which of these will grow and mature is not easy and may sometimes differ by sector or geography—or some may have a global impact. It is the difficulty with identification that makes preparing for these trends challenging.

Given that they take a long time to play out, preparation for these trends requires a long-term vision and strategic planning.

Many consultants and research bodies publish global trend reports aimed at trying to make predictions in different areas as to what the world will look like a decade or two into the future.[2] However, this is not an easy task, and the conclusions of different studies vary depending on the focus and vision of the authors and their organizations. As the famous Danish physicist Niels Bohr said, "Prediction is very difficult, especially if it's about the future."[3]

But notwithstanding this, it is necessary and prudent to attempt to study, evaluate, imagine and prepare. As famous science fiction author and futurist Karl Schroeder said, "Foresight is not about predicting the future; it's about minimizing surprise."[4]

By identifying emergence and preparing for it, organizations can minimize surprises.

Many trend reports identify several major areas of change and impact, including climate change; urbanization, inequality and inclusion; and demographic change. These examples give indications about the nature of emergence and how to prepare for it, but they are not exhaustive. Organizations need to watch trends and global reports and start preparing early to address these issues.

Climate Change

The tremendous developments made by humankind in areas such as infrastructure, industrialization, energy, transportation and farming over the last 300 years have dramatically improved quality of life. However, it has come at a high cost for the environment in terms of the effects of climate change, including rising temperatures, rising sea levels, the depletion of the ozone layer, and the pollution of air and water.[5]

This crisis affects the entire world, and it is imperative for everyone to do their best to act responsibly to minimize the effects of climate change. The United Nations *Sustainable Development Goals Report 2022* notes that:

> *As the world faces cascading and interlinked global crises and conflicts, the aspirations set out in the 2030 Agenda for Sustainable Development are in jeopardy. With the COVID-19 pandemic in its third year, the war in Ukraine is exacerbating food, energy, humanitarian, and refugee crises— all against the background of a full-fledged climate emergency.*[6]

Therefore, it is necessary for all organizations to address these issues no matter their business sector. Are they ready with a plan to become carbon neutral? What are they doing to consume energy more efficiently? Are they taking measures to stop pollution caused by their activities? Are they manufacturing products that support these causes? Are they publishing a verified environmental, social and governance (ESG) report that demonstrates their commitment to protecting the environment?[7]

The answers to these questions are important because customers use these considerations when choosing the types of organizations with which they wish to interact. Although these considerations may seem like a means to enhance an organization's image, in the future, such factors may determine their very existence.

Addressing this shift requires vision, strategy and commitment from the very top, including setting goals, declaring them, and making investments and efforts to achieve them. This is long-term work, but it should begin now.

Urbanization, Inequality and Inclusion

Populations are rapidly moving from rural to urban areas. This introduces both problems and opportunities for enterprises. More than half the world's population now lives in cities and towns, and by 2030, this number will reach 5 billion.[8] The increasing population density in urban areas strains the available infrastructure, but it also creates business opportunities for serving the burgeoning populations of cities with various goods and services.

However, the rapid pace of development has not showered benefits on everyone around the globe equally and uniformly. Disparities in standards of living vary grossly across populations. Including every person around the globe in development and its benefits regardless of race, color, caste, gender, nationality or any other criteria is an imperative for the world today. Society can sustain progress only together, not in pockets.

These issues have many social implications, and they will also impact organizations and their employees.

Demographic Changes

The global population is aging in most countries, and it is estimated that 22 percent of the global population will be older than 60 years of age by 2050—up from the current 12.3 percent.[9] Life expectancy is increasing due to better living conditions and healthcare services. The aging population decreases the share of people working and can lead to a shortage of resources in addition to the responsibility of caring for the aged.

Areas of Development

Some areas of development that could make an impact on enterprises and their use of technology include:

- **Quantum computing**—An emerging area of significant interest where much research effort is being expended is quantum computing. When quantum computing becomes technically viable and economically feasible, it will have the potential to completely revolutionize the world of computing. This new approach to

computing will not only significantly increase the speed and capacity for problem solving, but also transform how computers work. However, it will pose new risk areas and dangers as well. Will all existing encryption and cryptography become powerless at the hands of this brute compute power?[10] How will this change the technology that is currently used? It is important to stay aware of these new advancements.

- **Genetic and life sciences research**—Research in the areas of genetics and other life sciences aided by AI are heralding new advancements in healthcare. The benefits of this are better health and longer life expectancy. As mankind delves deeper into this domain, the risk of irresponsible use of some of the discoveries remains, which may impact many sectors and countries.

ROLE OF THE IS AUDITOR

Emergence should be addressed by senior leadership and the BoD. The role of the IS auditor in this area can be limited. The IS auditor needs to evolve from being an examiner, reviewer and verifier to becoming one who advises and guides as an expert. An IS auditor who evolves to this level is then given a seat at the table. An auditor has become a confidante of senior management and a valued adviser can participate in conversations or help develop processes regarding emergence issues for the organization.

CONCLUSION

The work and life of an IS auditor is exciting because the environment of business and technology in which auditors perform their work is changing dynamically— sometimes gradually but also sometime dramatically.

Recognizing this change is fundamental to the IS auditor's attitude, and preparing for this change is imperative for survival and success.

Interruptions, disruptions and emergence will continue to pose challenges to organizations, and IS auditors need to do their best to overcome these challenges. The weapon to fight interruptions is knowledge of existing technology, systems, processes and current methods and tools for prevention and mitigation. Disruption can be countered by learning about emerging technology and new innovations and tools. Continuous learning is an IS auditor's companion in the journey to keep pace with business and technology advances. An IS auditor who combines knowledge and their planning to keep pace with current events and trends with an attitude of being a partner in the organization, will get a seat at the leadership table to guide the organization on emergence issues as well.

EDITOR'S NOTE

The concept of emergence can have more than one definition. ISACA® defines emergence within its Digital Trust Ecosystem Framework (DTEF) as the arising of new business opportunities, new behaviors, new processes and

other relevant items as the subsystems between people and processes evolve. As spontaneous new ways of doing things emerge within an organization, they may be regarded as positive or negative. In some cases, emergence creates order out of chaos in unpredictable ways. For more information on emergence and the DTEF, go to www.isaca.org/digital-trust.

ENDNOTES

1 World Health Organization (WHO), "Weekly Epidemiological Update on COVID-19," Edition 114, 19 October 2022, *https://*www.who.int/*publications/m/item/weekly-epidemiological-update-on-covid-19-19-october-2022*

2 Koulopoulos, T.; "Four Megatrends Expected to Change Everything by 2050," *Inc.*, 11 March 2020, *https://*www.inc.com/thomas-koulopoulos/*4-megatrends-from-healthcare-to-changing-demographics-that-are-expected-to-change- everything-by-2050.html*

3 Anker, D.; "Forecasting—Prediction Is Very Difficult, Especially If It's About the Future," 7 October 2017, Crainfield University, *https://blogs.cranfield.ac.uk/ cbp/forecasting-prediction-is-very-difficult- especially-if-its-about-the-future/#:~:text=Niels%20 Bohr%2C%20the%20Nobel%20laureate,model%20out%2Dof%2Dsample.*

4 Schroeder, K.; "After Prediction," *https://*www.kschroeder.com/weblog/*after prediction#:~:text=Foresight%20is%20 not%20about%20predicting,not%20about%20 predicting%20 the%20 future.*

5 United Nations, "What Is Climate Change?" *https://*www.un.org/en/climatechange/ *what-is-climate-change*

6 United Nations, *The Sustainable Development Goals Report 2022*, USA, 2022, *https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development- Goals-Report-2022.pdf*

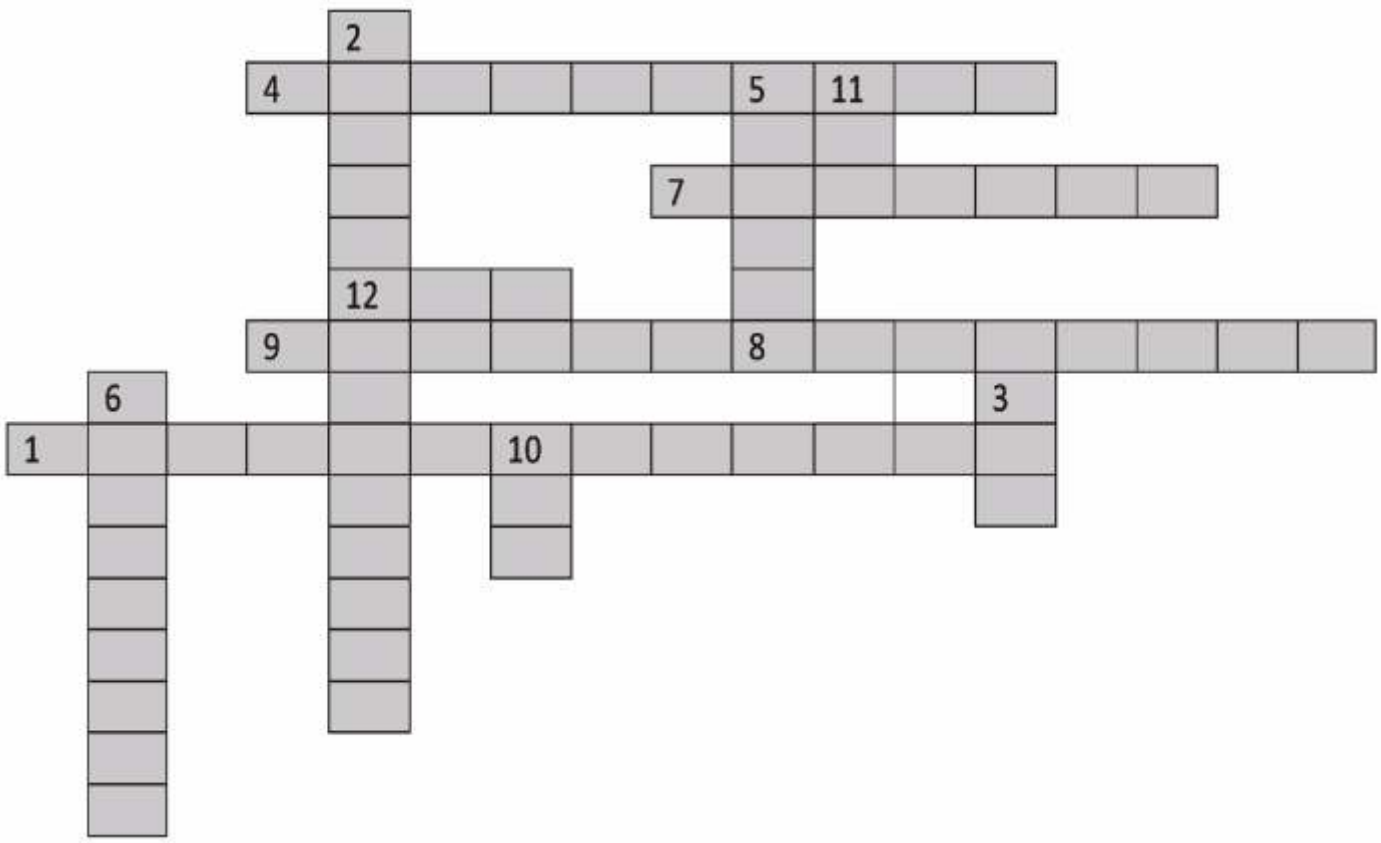
7 Tocchini, F.; G. Cafagna; "The ABCs of ESG Reporting: What Are ESG and Sustainability Reports, Why Are They Important, and What do CFOs Need to Know," Wolters Kluwer, 9 March 2022, *https://*www.wolterskluwer.com/ *en/expert-insights/the-abcs-of-esg- reporting#:~: text=What%20 is%20ESG%20 reporting%3F, organizations%20to%20do%20 the%20same*

8 United Nations Population Fund, "Urbanization," *https://*www.unfpa.org/urbanization

9 United Nations Population Fund, "Ageing," *https://*www.unfpa.org/ageing

10 Khader, D.; H. Siddiqui; "Making and Breaking Data Security With Quantum Machines," *ISACA® Journal*, vol. 4, 2022, www.isaca.org/archives

ISACA BANGALORE CHAPTER CROSSWORD PUZZLE



Across	Down
1. Symmetric Key Exchange Algorithm. (13) **4.** This is how strength of cryptography system is measured. (10) **7.** One way Encryption - Provides data integrity. (7) **8.** He developed AES. (8) **9.** Quantum bits used in Quantum Cryptography. (6) **12.** Combines hierarchy with "web of trust". (3)	**2.** Security Principle not supported by Advanced Encryption Standard - AES .(14) **3.** Jaya wants to communicate with Arun using symmetric key cryptography. How many key / keys she has to generate.(3) **5.** Roman King who used Substitution Cipher. (6) **6.** This occurs when change in plain text results in multiple changes in Cipher Text. (9) **10.** This hardware provideseffective way to manage encryption keys.(3) **11.** Most well known example of hybrid cryptography. (3)

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 August 15th, 2023.

Meeting with ISACA HQ Team

Intro Seminar held on 08-04-2023

Intro Seminar held on 01-07-2023

CPE Session held on 01-07-2023

STUDENT ACTIVITIES

The goal of ISACA Bangalore Chapter is to provide guidance and opportunities to students who are preparing for a career with a leadership role in all industries reliant upon and supported by information systems.

ISACA Bangalore Chapter is making every effort to involve Academic institutions and Students in ISACA activities.

Here we are trying to assist students and faculty from Jain college & Christ University by partnering with them to give students the opportunity to enhance their learning experience.

Intro Seminar held at Jain College on 05-07-2023

Intro Seminar held at Christ College on 08-07-2023

Makala Dhama Inauguration on 08.07.2023

COMMUNITY WORK

Supporting children's lives and empowering them to become happy and successful adults is one of the goals of ISACA Bangalore Chapter. To this end we opt to donate, volunteer, or attend any of the events organized by Orphans.

Three years back we launched the new volunteer initiative, ISACA CommunITy Day, which has now become an annual event.

We logged more than 250 hours of service and truly started a positive movement to change the world. Activities included digital security tutorials, mentoring orphans, donation of Clothes, Food and much more.

Here is attendance of one of the events organized by Orphans.

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