Q1 - 2022 ISSUE

ISACA
Bangalore Chapter

InfocITy Auditor

ISACA Bangalore Chapter - News Letter

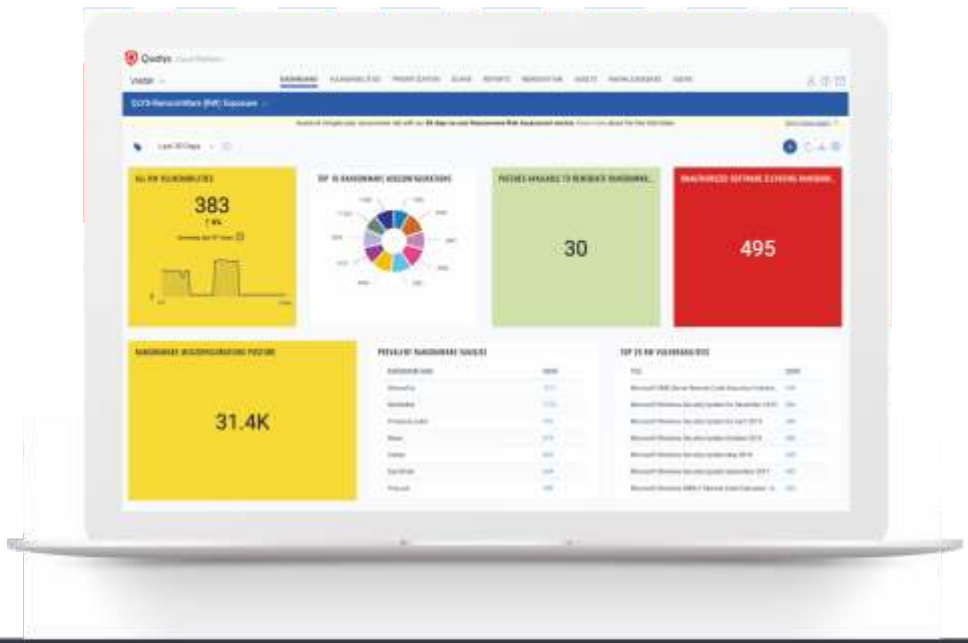
Qualys.

Ransomware Risk Assessment & Remediation Service

How Vulnerable Is Your Organization?

Find Out Today with a 60-day No-cost Trial from Qualys.

Ransomware attacks are the most serious, fastest-growing cyber threats facing businesses today. These attacks are becoming more sophisticated and difficult to deter day-by-day. Trouble is, despite guidance from key industry organizations and plenty of prevention tips from security vendors, there's still no comprehensive, research-driven strategy for evaluating ransomware risk exposure and developing a prescriptive remediation plan. Until now.



Qualys Ransomware Risk Assessment & Remediation
Try it today at no cost for 60 days.

Visit qualys.com/ransomware

india-info@qualys.com

CONTENTS

ISACA Bangalore Chapter

InfocITy Auditor

Q1 - 2022

From The Desk Of The President

Dear Members,

Greetings and thanks for renewing your 2022 membership. Every year your membership elevates you to a new tier (Bronze, Silver, Gold and Platinum) with greater rewards and access to exclusive tools and insights which helps you to excel even more in your role.

The Chapter has grown as always and we are glad to see that we have crossed 2000+ members. This shows the Trust and the Confidence that you all have instilled in us. We will do everything that is required to keep the Trust and Confidence in tact.

We have been able to conduct regular CPE / SLB sessions with the active participation coming from each one of you. To name a few: 'New Frontier of Data Protection and Cyber Security', 'India's Data Protection Bill: Fundamental Business Impacts', 'Stress Management and Mindfulness' as one of the offbeat session based on the request from many of you. We called in for the Women Leaders to talk through their journey, the achievements, the challenges they faced. It was a great panel discussion held on 12th March, as part of our SheLeadsTech initiative to commemorate the International Women's Day (March 8th), the topic that we chose was "BreakTheBias – Impact to post-pandemic / endemic World' and it was an excellent session by our panel members.

We see the World opening up slowly after a long pandemic gap and a lot of us are working towards going back to office, as part of the 'Return to Office' (RTO) strategy. While the RTO is happening on one side, we still need to ensure, we continue to maintain certain precautious safety measures - wearing a mask, safe distance from one another, washing hands frequently, using hand sanitizers etc… We all hope and pray for the pandemic to end soon. We have faced the difficult times, however not out of it completely and hence it is important that we stay safe and healthy.

We are still connecting with our members via the virtual mode and provide as much value as possible. We will be releasing the 'white paper' contest shortly and hence request all of you to stay active in looking through our communications. We also call for Members to come forward and share any articles that they want us to publish in our newsletters. We are also planning engage our Members in supporting us to conduct some of the events, which will also enable us to motivate some of you to come forward and be a part of the Board. Also, share with your friends, family and colleagues about the review classes, the CPE / SLB sessions and various other value adds provided by us – the "ISACA Bangalore Chapter"

We are close to our Annual Conference time and we are planning to conduct an offline (in-person) conference, provided the situation gets better than where we are today. This will be our 25th Annual Conference and want to conduct this in a grand style. We are preparing for the same and will share inputs shortly and as usual expect all your active participation. Watch this space for more information in the near future.

As always, we solicit your active participation in the Chapters events and initiatives including monthly CPE meetings, SLB, Newsletter article contribution, Review Classes for aspiring students and more.

Looking forward to meeting you all in the next event either Physically or Virtually !!!

Warm Regards,

VELMURUGA VENKATESH, CRISC, CDPSE, ISO 27001 LA, ISO 31000 CRM, COBIT-5 (F)
President

Message From the Vice President

Dear Members,

Greetings!!

Many thanks for the renewal your 2022 membership and certification(s), we are sure that all of you are getting continuous benefits and support from ISACA HQ and our chapter. Two outstanding sessions were delivered as part of CPE on India's Data Protection Bill: Fundamental Business Impacts and Emerging Technology and Cyber and we are sure you have enjoyed the sessions, chapter also hosted three SLB sessions as of now for our members in the year 2022.

As part of SheLeadsTech program in March, an online event with leading women speakers from various industries as part of the International Women's Day celebrations was held.

Thank you once again for the renewal of your ISACA membership and certification and for supporting the chapter to maintain the leading chapter in terms of membership.

Now the pandemic-related news has reduced and is business as usual for all of us. Fortunately, the impact of the third wave did not create any havoc in the country. But a war started as the world watched in disbelief, Russia President authorised military troops to carry out attacks in Ukraine. At this point, there is no end in sight to the Russia-Ukraine crisis that has drawn and could draw more nations into the battle. In an era where nations are interdependent in many ways, any form of war would have far-reaching consequences.

Many websites were probably attacked by DDoS: an excessive number of requests per second was recorded. Ukrainian government's Center for Strategic Communications, Private Bank faced a "massive DDoS attack" that blocked many online banking services, including payments and balance inquiries. Last month, state-sponsored hackers launched a "massive cyber-attack" on Ukraine, shutting down several government websites. Various Ukraine 'websites of the Ministry were down due to cyber-attack. This shows the importance of the cyber security preparedness required for the war-like situation.

We can hope wisdom will prevail and both countries move to negotiate the table and put an end to this current turmoil in world peace. The world is still reeling from the Covid-19 pandemic, which hurt the poorest countries and people the most. Hope to see there will not be any more Escalation.

I'd like to take this moment to thank you all for your support and I also wish you and your loved one's health and safety.

Regards,

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

Message From Secretary

Dear ISACA Bangalore Chapter Family,

I would like to take a moment to reflect on the invasion of Ukraine and to express our support for all members of our community who are affected by these events.

We have overcome so many challenges these past two years and changed numerous lives. It brings me great joy that we have worked so hard this year to grow. The result has been excellent growth in membership. Let us keep up the momentum. I am happy that you have put a spotlight on all we do. The future looks brighter than ever for our Chapter and more than 2000 members. I appreciate your engagement and your commitment to our Chapter and to one another as we venture forward together.

I am grateful to every member of this community for the tenacity, resilience, capability, and pride that you have demonstrated as we came together not merely to push through this long ordeal, but to sustain and build upon our exceptional culture to promote the education, expand the knowledge and skills of members in the interrelated fields of IT governance, IS audit, cybersecurity, privacy, control and assurance.

ISACA Bangalore Chapter has long been a place that brings together bright minds to address the issues of today and look forward to what may come in the future. Recently, Bangalore Chapter was privileged to commemorate the cultural, political, and socioeconomic achievements of women by hosting Panel Discussion on “BreakTheBias – Impact to post-pandemic / endemic World” and web-based SLB session “Stress Management and Mindfulness” …. a celebration of International Women's Day (IWD).

Regards,

VIJAYAVANITHA, MBA, M. Com, CISA, CIA
Secretary

Renewal of your ISACA membership for 2022

Warm Greetings from ISACA Bangalore Chapter! **Wish you and your family a happy holiday season and Happy New Year !!!**

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.

Now it is time for renewing your ISACA® membership for 2022 if not already done. Please ensure to renew your membership before the PURGE to ensure the benefits arising out of continued membership.

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: **$10.00**
Total Dues for 2022 membership renewal: **US$ 145.00**

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

NervioCloud
Rationalizing Data Clouds

NervioGuard®

Ransomware lockers for NAS, File servers and Databases

NASSCOM Emerge 50 Awards 2019

NASSCOM DeepTech Club Mentee

Patent # US9128626

Reach us…

Mail: info@neridio.com

Visit: www.neridio.com

Part of NASSCOM Deep Tech *Club* Cohort 3

*"We live in the world of Cyber-attacks, ransomware onslaught, data breaches, insider-attacks and various IT disasters. Financial/Insurance institutions, defense, high-tech and healthcare organizations facing a daunting challenge - keeping their NAS Systems containing the backup storage infrastructure and critical data like EMR/PACS data stored in data servers or customer data stored in databases like MySQL or MongoDB under full visibility, security control and safe from intruders. Modern day digital infrastructure needs new approach to ransomware attacks – **NervioGuard®**, just delivered that on its market pioneering mission'' with its multi-vectored ,ransomware Risk mitigation solution.*

NervioGuard®

Swiss-army knife of ransomware mitigation - a revolutionary data fabric software that deeply converges data security, visibility and protection controls, targeting NAS systems, MySQL and NoSQL databases.

Patented data security technology built over decades of research and development.

Fully deployable On-Premise or in Hybrid / Multi-Cloud environments.

World's first integrated solution that has multiple layers of security and protection intelligence. This is the single solution that can detect, mitigate and recover with attack avoidance data platforms.

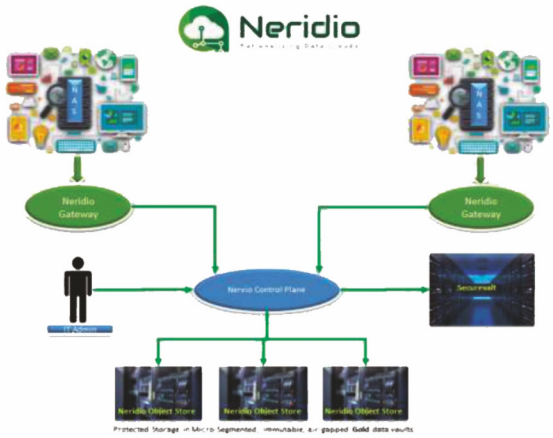
Real-time storage intrusion detection and active incident response mechanism with novel orchestration of AIOps, ITOps, SecOps paired with integrated data virtualizations and protection services.

A truly secured data protection platform with unified backup and archiving services for corporates offering cyber resilience, GDPR compliance and Ransomware Protection.

Zero Trust architecture together with ransomware aware technologies, NervioGuard® ensures data Safety and Security by Design.

Security and control of the solution can optionally be augmented by a SaaS service providing contextual Risk mitigation and Autonomous security control.

"Ransomware worms attacking corporations of all sizes. CSOs/CIOs are paralyzed by the threats of various natures that ravage their IT systems and question the very existence of their businesses. There isn't a single solution that offers a holistic integrated approach on detection, mitigation, recovery and avoidance''.



How it works?

NervioGuard transparently copies active files, archives cold files, based on customer-controlled data classification policies from existing NAS systems into Nervio Gold Copy infrastructure, which was built with ransomware Risk mitigation by-design. All files are classified based on data privacy policies and business value. The data, then compressed, de-duplicated, encrypted without any key management hassles, erasure-coded based on the Reed-Solomon dispersal algorithms and distributed with N:M (such as 2-3 or 3-5) availability across multiple storage vaults in private or public clouds. This unique approach realizes an unmatched moat of cyber resilience and ransomware protection. NervioCloud data vaults are Securely Isolated from the network. Data can be instantly accessed, at drive level to any point in the past.

Advantage and Benefits

- Radical simplicity and Security for Backup infrastructure hosted in NAS systems or Databases with multi-vectored Ransomware resilience with any point, instant data access from ransomware-tolerant snapshots.
- Un-hackable Ransomware lockers with Data dispersed across multiple locations with secure network isolation delivering un-matched ransomware resilience.
- Centralized Security Surveillance and Intrusion response against abnormal systems or storage activity due to potential ransomware infection across multiple sites.
- Built-in ransomware recovery support with the integration of private storage clouds through multi-cloud storage virtualization technology for un-hackable security barricade against cyber-attacks or insider threats.
- Multi –Segmented data vaulting with logical air gapping for ransomware immunity.
- Enables Data Compliance and Data Governance by converging various data and security services Across IT silos.
- Auditable storage accounting for storage activity surveillance.
- Autonomous Risk mitigation in real time.
- Contextual data protection in real time, During the Attack.
- End to end - Pre-During -Post attack mitigation for Ransomware

Recap of Chapter Programs in Q1, 2022

CPE Sessions:

1. Topic : "New Frontiers of Data Protection and Cyber Security"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 8-Jan-2022 (Saturday) Time : 6:30 PM - 7:30 PM IST
1 CPE Credits offered

The paradigm of a frontier fits very well with what is happening in the world of tech-led banking. There is a frenetic activity akin to the gold rushes of the 19th century.The first frontier is that of data protection. It cannot be denied that the entire FinTech innovation proposition is based on the exploitation of willing/inadvertent data sharing of the users, bypassing data protection and privacy principles. With only token consents being collected through browse-wrap/click-wrap forms, the informed aspect of the consent collection is subverted. This space will need to be watched, especially with India's Data Protection Act on the anvil.

Speaker Profile: Mr Nandkumar Saravade, Founding CEO of Reserve Bank Information Technology Pvt Ltd. (ReBIT)

Mr Nandkumar Saravade is a senior advisor on governance, strategy, ethics and cyber security. Drawing from his impactful stints in government and private sector spanning 36+ years, with expertise across diverse domains of law enforcement, banking, cyber security and technology management, he considers himself a 'knowledge-seeker with action-bias.' Mr. Saravade was the founding CEO of Reserve Bank Information Technology Pvt Ltd (ReBIT). ReBIT was set up in 2016 as a fully-owned subsidiary of RBI for technology management and cyber security for RBI's systems and the Indian banking sector.

2. Topic : "India's Data Protection Bill : Fundamental Business Impacts"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 22-Jan-2022 (Saturday) Time : 5:30 PM - 7:30 PM IST
2 CPE Credits offered

The Indian Data Protection Bill impacts organizations in ways that are yet to be fully comprehended by most business persons. Many assume it is limited to Security. This talk endeavours to give an overview of what implications the forthcoming law will have on business operations overall.

The following would be discussed:

- Implications of the DPA for Organizations
- A basic approach to address the challenges thrown up
- High-level learnings from the experience of other organizations

Speaker: Shivangi Nadkarni, Co-Founder & CEO - Arrka

3. Topic : "Emerging Technology and Cyber Security"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 26-Feb-2022 (Saturday) Time : 5:30 PM - 7:30 PM IST
2 CPE Credits offered

IT is no more a support function but a business enabler. Emerging technologies like AI, Robotics, IOT are changing business operations. Should we be worried about them? What are the consequences we can see for the same? Can we use them for security as well to strengthen our Risk Posture?

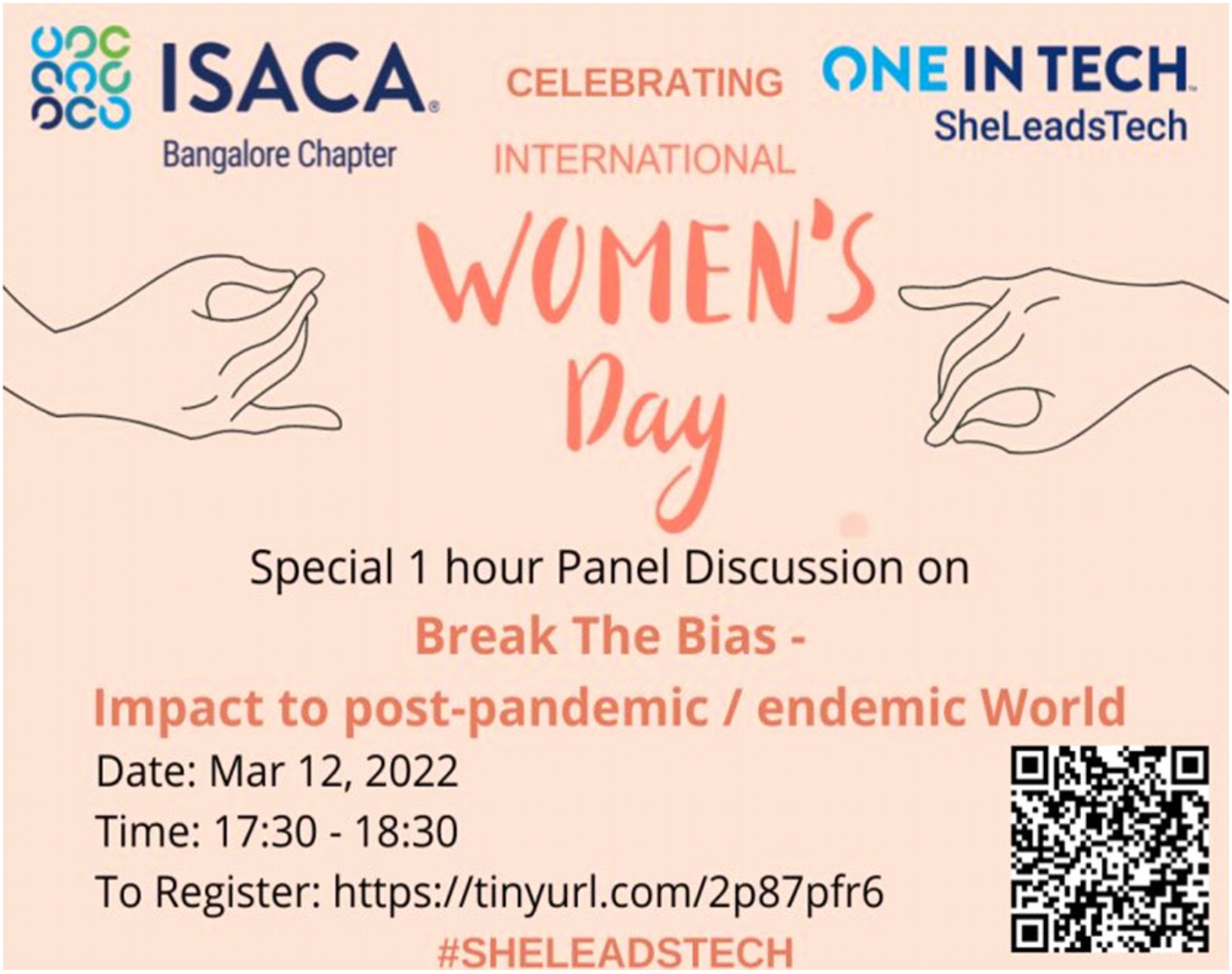
The session would cover the following:

- How to effectively use Emerging Technologies in our business.
- Risk Associated with new-age Digital Revolution
- Using emerging technology as Cyber Security Tool.

Speaker: Mr. Gaurav Batra, Founder & CEO - CyberFrat

4. Topic : "Special Panel Discussion on 'BreakTheBias' and Online Introductory Seminar on ISACA Certifications"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 12-Mar-2022 (Saturday) Time : 5:30 PM - 6:30 PM IST and
6:30 PM - 7:30 PM IST Online Introductory Seminar on ISACA Certifications
1 CPE Credits offered

Special 1 hour Panel Discussion on 'BreakTheBias - Impact to post-pandemic/endemic World (from 5.30 pm to 6.30 pm)



5. Topic : "Stress Management and Mindfulness"
Venue : Web-based ONLINE session via Zoom Webinar Platform
Date : 19-Mar-2022 (Saturday) Time : 5:30 PM
2 CPE Credits offered

Little stress is motivational, a lot of stress damages health, relation, and an organization. With the right management strategies, one can reduce the amount of stress in life and organization. Learn how to identify and access your stress triggers, manage response, more effectively, and make positive personal choices for organizational benefit.

The session would cover:

1. Understand Stress, its causes, and impact
2. Neuroscience of stress and science-based techniques for Stress Management
3. Mindfulness techniques to manage stress anywhere and everywhere.

Speaker: Neetu Choudhary, Professional Speaker & Life Coach

OUR PORTFOLIO

30 FULFILLING YEARS

VALUE POINT
VALUEPOINTSYSTEMS.COM

Cybersecurity

- Endpoint Security Practice
- Network Security Practice
- Data Security Practice
- Cloud Security Practice
- Governance, Risk & Compliance
- Security Operations & Automation
- Managed Security Services

Data Center Modernization

- Hyper Converged Infrastructure
- All Flash Storage
- Virtual Desktop Infrastructure
- Remote Applications Access
- Software Defined Storage
- High Performance Blades
- Disaster recovery & Backup Solutions
- Kubernetes & Containers
- Private Cloud Solutions

Network Transformation

- Wifi Solutions
- SD WAN
- Switching
- Routing
- Structured Cabling
- Electrical Contract
- Meeting Room & Conferencing Solutions
- Internet Of Things (IOT)
- Network Monitoring
- Network Assessment & Consulting
- Data Center Design & Build
- Electronic Security & Automation

Cloud Transformation

- DevOps Services
- Migration Services
- Cloud BCP & DR
- Cloud Security
- Cloud Optimization
- Cloud Managed Services
- VDI On Cloud
- Data & Analytics

Digital Workplace

- Compute - PC | Laptops | Workstations | Thin Clients
- Display - Kiosk | Video Walls | Digital Signages | Projectors
- Print - Copiers | Plotters | Printers | Scanners | Toners & Ink
- Solutions and Services - Mobility | Display | Digital Workflow

IT Managed Services

- Warranty Support
- AMC Support
- FMS/ IT staffing
- ITSM Tools
- NOC Support
- Hybrid Support
- Professional Services

+91 78999 00121 | reach@valuepointsystems.com

#fulfillingyourfuture

Cloud Computing Trends For The Year 2022

- Chetan Anand, CDPSE
Associate Vice President - Information Security and CISO, Profinch Solutions

About the Author:

CHETAN brings over 18 years of professional experience in information and cyber security, business continuity, privacy, risk and quality. He has worked in various industries such as IT, ITES, Fintech, Healthcare / Pharma, Manufacturing, Research and Development, in various capacities including Technical, Managerial and Leadership roles. He has contributed to the ISF's research on Continuous Supply Chain Assurance, report review and functionality testing of ISF tools. He is a member of and volunteers with ISACA. He is an ISACA Global Mentor, is on the review panel of ISACA Journal and has contributed to ISACA whitepaper and blog. He possesses various certifications to his credit including CDPSE, Fellow of Privacy Technology, NLSIU Privacy and Data Protection Laws, CPISI, CCIO, ISO 27001 LA, ISO 22301 LA, ISO 31000, ISO 27701, ISO 9001 LA, ISF IRAM2, SQAM, Lean Six Sigma Green Belt, Agile Scrum Master etc.

As we welcome 2022, it can be a valuable time to explore trends that may impact the IT industry. Let us take a look at those trends specifically related to cloud computing, given its increasing importance today.With the global impact of COVID-19 pandemic, many organizations have opted for online and hybrid models for their work environments. Information technology assumed centre stage with new technologies that were harnessed to its their full potential to keep the wheels of the economy moving. The need for online collaboration increased within organizations and with external parties such as customers and suppliers using cloud technology.

While cloud has made life a lot easier, it is still in its nascent stage in India and continues to evolve with each passing day. One of the biggest challenges that cloud computing poses is the threat of hacking, although there are numerous options available to protect data from external threats and attacks.

As cloud computing continues to evolve, I foresee a few trends that will define the space as we enter 2022.

New Use Cases

2020 and 2021 witnessed large adoption of virtual meeting applications. With the buzz around 5G and Wi-Fi 6E gaining momentum, this means that more new types of data can be streamed. Studies and expert opinions reveal that the arrival of cloud virtual and augmented reality (VR/AR) can lead to cheaper and smaller headsets. With this cloud technology, every other technology becomes faster, lighter and more accessible to the end user, which will propel more services migrations to cloud platforms.

Hybrid Cloud

As the name suggests, this upcoming year could witness increased adoption of multiple cloud platforms – private and public. The combination of hybrid cloud will be used to allow workloads to juggle between public and private clouds, giving clients greater adaptability.

Zero Emissions

Per the World Economic Forum, the next big cloud competition is the race to zero emissions. Cloud computing and data centres have become core global infrastructure – the roads and bridges of the internet economy. But they've also become a significant driver of carbon emissions, responsible for an estimated 1.8% of US electricity consumption and the plurality of emissions for many tech companies. Google is working towards 24/7 clean power for its data centres, Amazon is shooting for 100% renewables by 2025, and Microsoft is leading the way on transparency for its cloud customers. But these targets are just the beginning. Cloud computing and data centres are responsible for the majority of emissions for many tech companies, creating competition to provide cleaner cloud services. The

more savvy and transparent corporations get about their carbon footprint, the more pressure they'll place on major cloud providers to accelerate the road to zero carbon.

Cloud Audits

Upskilling is necessary for everyone no matter how many years of practical IT experience you have on your team. One of the areas that will become even more important to gain training and knowledge in is cloud audit, as cloud auditing is essential to effective cloud management. ISACA, a global leader in training, education, and certification for information security and information technology professionals in association with Cloud Security Alliance, a global leader in cloud security research, training and credentialing, offer the Certificate of Cloud Auditing Knowledge (CCAK). CCAK is the first-ever, technical, vendor-neutral credential for cloud auditing. This certificate fills a gap in the industry for competent technical professionals who can help organizations mitigate risks and optimize ROI in the cloud. CCAK prepares IT professionals to address the unique challenges of auditing the cloud, ensuring the right controls for confidentiality, integrity and accessibility and mitigating risks and costs of audit management and non-compliance.

Changes to ISO 27001 and ISO 27002 Standards

Organizations will also need to ensure they are complying with the latest standards that relate to cloud services. Professionals should pay close attention specifically to ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems and the ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls standard, which are both undergoing changes.– The latter will become the "Information security, cybersecurity and privacy protection - Information security controls." As per the ANSI National Accreditation Board in the US, twelve new controls will be introduced in these standards, including *information security for use of cloud services.* This means organizations that are certified for the ISO 27001 information security management system standard need to gear up to implement this new control related to cloud services.

Serverless

Cloud computing envisages a design where businesses access IT infrastructure on-demand without the need for any investments on servers and infrastructure. Serverless is a subset of PaaS, which needs more processing power, but in intervals or bursts. Serverless cloud is also used by companies that are developing new applications but lack the resources to deal with the required infrastructure.

Automation

A key element to cloud computing is automation. With data and systems on a centralized cloud, companies can automate many of their internal processes - be it data consolidation from different sources or business intelligence dashboard creation. Organizations today are looking to tighten connections between different pieces of software and make sure that solutions from multiple vendors work seamlessly.

Edge Computing

With over thousands of IoT devices connecting to the internet every second, organizations are bound to face security, latency and bandwidth issues. And when organizations use more advanced technologies like robotics and artificial intelligence, the need for more power and faster processing increases. Going forward, organizations will decentralize the entire cloud environment and create localized data centres that offers readily available storage and computing power near places where it they are needed.

As dependence on cloud continues well into 2022, the complexity of the cloud environment will also grow and continue to challenge businesses to innovate and find newer ways to harness its full potential, as well as to provide their teams with relevant training and credentials to stay up-to-date with cloud knowledge and trends.

Significance of Risk Culture in an Organization

- Udayshankar Tadigadapa

About the Author:

UDAY is an experienced professional and manages various risk management functions and activities for the firm. He works as Vendor compliance manager with Diageo.

What is risk-based culture?

First let us understand the word risk. Similar to the various definitions we can find for culture, risk too has no single meaning. Risk can be defined as 'Potential events that may impact the entity' or 'effect of uncertainty on objectives' or 'a situation involving exposure to danger' etc. A risk-based culture or organizational risk culture can be defined as 'conscious behaviour which aims to continuously identify potential events which may adversely impact business objectives and taking appropriate measures to reduce or nullify this impact'. The quantum of risks we see today are not the same before. Today's organizations and the business landscapes have evolved after the many revolutions such as industrial, scientific, quality, and digital. In the 1970's there was a fierce competition between the western product manufacturing companies and those from Japan majorly. The focus was on vying for the maximum market share by acquiring customers through great quality goods. Just-In-Time (JIT) or Kanban, 5S, Kaizen, 6-Sigma, Total Quality Management (TQM) and various other quality systems and methodologies were invented and adopted after they showed promising results.

Then the focus was highly on producing good quality goods but still the markets were not as integrated as they are today. Customer base was limited to a country or a few countries which had clear trade agreements between them. Hence the exposure to risks were also limited to a comfortable extent. But this changed. The spur of Information Technology gave birth to the digital revolution where records, financial information, sales orders, invoices, customer databases and so much more slowly started getting digitized and the internet connected the whole world in a manner which was unprecedented. That's what Thomas Friedman's book 'The World is Flat' explains. Globalization shifted the focus from locally producing good quality goods for a limited customer base to extending the product life span and simultaneously lengthening the customer experience through a service-oriented business model, now at a global scale. All enabled because of Information Technology.

However, with this integration and digitization the businesses got exposed to many new risks and opportunities too. With the expansion of customer markets came increased demand and so supply too had to be increased. Sourcing raw materials and producing locally for local or geographically near markets was no longer a viable solution. Organizations had to spread out manufacturing units to save on logistical costs and service the customers more efficiently.

Natural calamities such as floods, snowfall, earthquakes, landslides etc. which companies were not exposed to earlier emerged as major risks disrupting supply chains and hence Business Continuity Planning (BCP) became a necessity. In addition, regulatory, financial, legal, operational, logistical, reputational, and of course information security and cyber risks complemented with privacy risks, due to the massive increase in digitized personal information, started to collectively impact companies worldwide in unknown ways. This mandated a steep learning curve. Companies which adapted and learnt how to deal with these risks just survived or perished and those which not only learnt to deal with the current risks but also learnt to identify potential risks in advance and prepared, emerged as leaders in this globalised world.

Those organizations which realised the importance of risk management and made this an integral part of their day to day and strategic planning ushered in a risk-based culture which helped them not only survive but maintain the required market share to retain the leadership positions.

Survivors and The Leaders

What has just been described is how the risk landscape evolved and how organizations too had to embrace change to survive. Since risks constantly evolve and organizations, individuals, and countries too need to adapt to just survive or to lead. Here are some examples which will throw further light on the relationship between keeping the risk culture intact and survival or leadership.

Fannie Mae formally known as the Federal National Mortgage Association (FNMA), was a United States of America's (USA) public sector enterprise. Its role was to lend money to local banks who in turn lent to home buyers. It was started post the Great Depression in the 1920's as an economic revival measure. Over the decades Fannie Mae emerged as a leading financial institution in the USA. It featured multiple times in the top echelons of the Fortune 500 list and even as one of the great companies in the famous book 'Good to Great' by Jim Collins. However, when the subprime mortgage crisis hit USA's financial markets Fannie Mae spiralled down the performance ladder as if a snake had gobbled it up in a snake & ladder game. So, what happened?

Fannie Mae's debacle was a result of a lack of oversight from central regulators over the private financial institutions and even within the public sector financial institutions the pressure to meet lending targets amidst the stiff competition being provided by the private players came at the cost of proper risk management. It would be unfair to say that there were no risk management practices in place at Fannie Mae but the fact that the crisis revealed the lack of sufficient oversight should raise the question as to whether the organization had a strong risk-based culture or not.

On 15 th July 2020 Barack Obama, former president of USA, tweeted that he would double the money paid to a particular Bitcoin account and that it was his way of giving back to the community during Covid-19. The catch here is that it was not really Barack Obama tweeting this, but it was the real Twitter account of Barack Obama from which this tweet originated. It was later found that a 17-year-old individual orchestrated an intricated spear-phishing campaign and certain Twitter employees fell into the trap. The situation was controlled but it could have spiralled into something more drastic, possibilities were scarily many.

Investigations revealed that mid-level employees were the initial targets and after gaining access to tools at that level and subsequently with well-planned reconnaissance, the attackers gained privileged access to the high-profile accounts. Clearly, unguarded human behaviours were exploited, and rest is history. As one of the correction measures Twitter stated that their efforts to improve upon pre-existing security systems and processes will increase to avoid such incidents in future.

Inherently though, continuous risk identification and awareness, training, communication, timely remediation, and proper oversight to prevent incidents need to be fortified based on a strong culture of risk management. At any point if an organization and its employees think that they are invincible becomes an antithesis to an effective culture of risk management. A good culture of risk management will not only prevent major incidents from occurring but should help the organization to control the spread of damage further and make it bounce back to normalcy faster.

Almost 1,500 earthquakes of varied magnitude strike the land mass of Japan each year. Apart from this there are typhoons, landslides and floods which cause damage to life and property consistently in Japan. Still, we know that it is one of the successful nations of the world in almost all domains of life. The culture of risk management is ingrained in the overall culture, this is one of the finest examples of risk management being integrated within the regular way of life. Centuries of living with these natural risks have taught the Japanese to become resilient and proactive in managing the risks. They have developed state of the art weather forecasting and meteorological

advance warning systems which helps in reducing loss of human lives. Continuous awareness programs on safety and survival drills keep the citizens mentally prepared to handle the calamities better. Good communication protocols and mediums have been developed to make the necessary information available in time for example where are the safety zones and how to reach these places. The skyscrapers in the major cities are built using technology which make them earthquake resistant. At the same time the research in making the existing predictive and disaster management systems even better continues unabated.

The Essentials of a Risk Culture

So, what could organizations be doing to develop and then assimilate an effective risk culture as part of its DNA? Similar to not having a one size fits all definition for culture or risk, there is no standard set of rules or guidelines here however based on examples such as what organizations did or are currently doing right or wrong in this regard would be helpful to understand and adopt.

The reverse iceberg model:

The iceberg as we know has 1/4 th of it visible above the water level and 3/4 th submerged. If good risk management practices are to get ingrained into the organization's culture, then there must be a commitment from the top management. That is why the analogy of the reversed iceberg is being used here. It should not be that top management commits only 1/4 th of time, resources, and interest towards building a risk culture and perhaps more is required only then the other employees will follow and reinforce the risk-based culture.

Great design needs to be backed up by greater execution:

Many organizations have splendid risk management policies and engage big consulting firms to help them design the risk management program. However, continuity and again commitment is essential. Many risk management initiatives and projects get stalled mid-way and budgets are not replenished. It takes months or even years for the stalled initiatives to be revived and again the need to validate with market or peers would require engagement with consulting firms so again more costs with no returns. Starting small and fail fast should be the mantra to progress faster towards building the risk-based culture. You do not need a grand plan to do this, start with the basics for example hire a small team of experts, let them start putting the vision and objectives into action and from there grow gradually into a more mature risk organization and process.

Certainty is a mirage:

Risk culture needs to be based on dynamism and there is no place for stagnation or laziness. An organization firstly should maintain a risk register with 'relevant' risks i.e., those which are related to the business and which can negatively impact. Secondly this risk register should be a living document. So legacy risks should be revisited regularly, and this can be done through an oversight program, also new risks identified periodically should get added to the risk register. Risk register is only one example, consider these scenarios also -

An Intrusion Detection System (IDS) relies on certain algorithms to detect malicious content being pushed into an organization's network. Having false positives i.e., content being categorised as a potential threat when it is not is a less risk however false negatives i.e., an actual threat being categorised as safe content and being allowed into the network is a strict no-no. So, unless an organization takes care and that extra effort to update the IDS regularly with vendor patches which sometimes can update the detection algorithms based on the recent threats identified and inspect the logs from time to time to see that things are working the say they should, blindly believing in the risk management tools is also dangerous. This concept has been beautifully and elaborately explained in the book 'Risk Savvy' by Gerd Gigerenzer.

Sometimes it is the haystack, which is the problem, not the needle:

Having the right strategy plays a very important role. Strategic risk needs to be taken care of primarily. Many organizations today have varied processes of which many could be so irrelevant to the core business itself. They operate in markets which do not contribute much to their top or bottom lines. The roles performed by individuals

in the organization are not linked with the vision or mission. Especially the centralized support functions do not operate like a central function. There would be one CIO for the organization however his or her influence on a local markets way of functioning would be almost zero which allows the local head of business to authorise a tailor-made IT strategy, you can imagine the disparity it would invite thus exposing the organization to serious reputational risk and many other risks. These areas need constant review and realignment right from the top. Only when the business is sorted the risks which we identify are relevant, consistent, and hence managing these would keep the organization safer.

Do not boil the ocean:

The flipside to all this is overdoing risk management. Risk culture must be sustainable. Apart from regulatory requirements some organizations mandate excessive trainings, certifications and encourage multiple internal audits that the risk owners experience fatigue very soon. Risk owners usually have another day job to perform but they get so overburdened by these requirements that their job satisfaction levels and commitment to the risk culture can reduce. Balancing risk culture with the needs of individual roles is an art.

Risk is everyone's business, but ownership needs to be assigned:

On one hand it is advised to not burden the risk owners with too much of tasks however it is very important to clearly define risk ownership. As stated, balancing risk culture with the requirements of individual roles is an art. The lines of defence can get blurred if accountability to risk, roles and responsibilities are not clearly defined and communicated. Risks can get tossed like hot potatoes from one individual to another and in this process the risk is not resolved or treated appropriately.

Competencies are key for those enabling risk management:

Organizations which have invested in risk management roles need to ensure that the individuals filling those roles are competent to be performing them. Risk culture is a new area and individuals who have a thirst for knowledge and are consciously upgrading their skills are necessary to keep the risk culture alive and thriving. Not always individuals hired externally bring what is required to the table and motivated existing employees can become great risk professionals if they are provided basic training and are given a direction as to which areas of skilling they need to achieve. In fact, this could enhance the loyalty factor within these individuals and would serve the organization in its best interests. So, a healthy combination and rotation of internal employees, external consultants and newly hired risk professionals can constitute the perfect team for the organization.

Conclusion

Risk is not an easy subject. The uncertainty makes it opaque and only a constant vigil to identify the right risks, preparing well to counter the risk, continuous oversight and building resilience to bounce back to normalcy can help manage risks better. That is why a risk culture becomes so pertinent because culture is intrinsic and deep rooted, so once it is embedded the organization develops sort of a defence mechanism against serious losses. Its is like saying the vaccine may not prevent someone from catching the Covid-19 virus but it would lessen the chances of getting admitted in an ICU or from something even worse. Regarding Covid-19 a culture has evolved in the world. Wearing masks, social distancing and getting vaccinated have almost becomes synonymous with common human behaviour and God knows this may not go away from our lives any time soon.

Keeping the essentials of risk culture in purview will help but again each organization or anyone aiming to build an effective risk culture should put these into context and implement, improve, or do something totally different that suits the case. But acknowledging the need for enabling a risk culture is the first step, a universal lowest common denominator and this is most important.

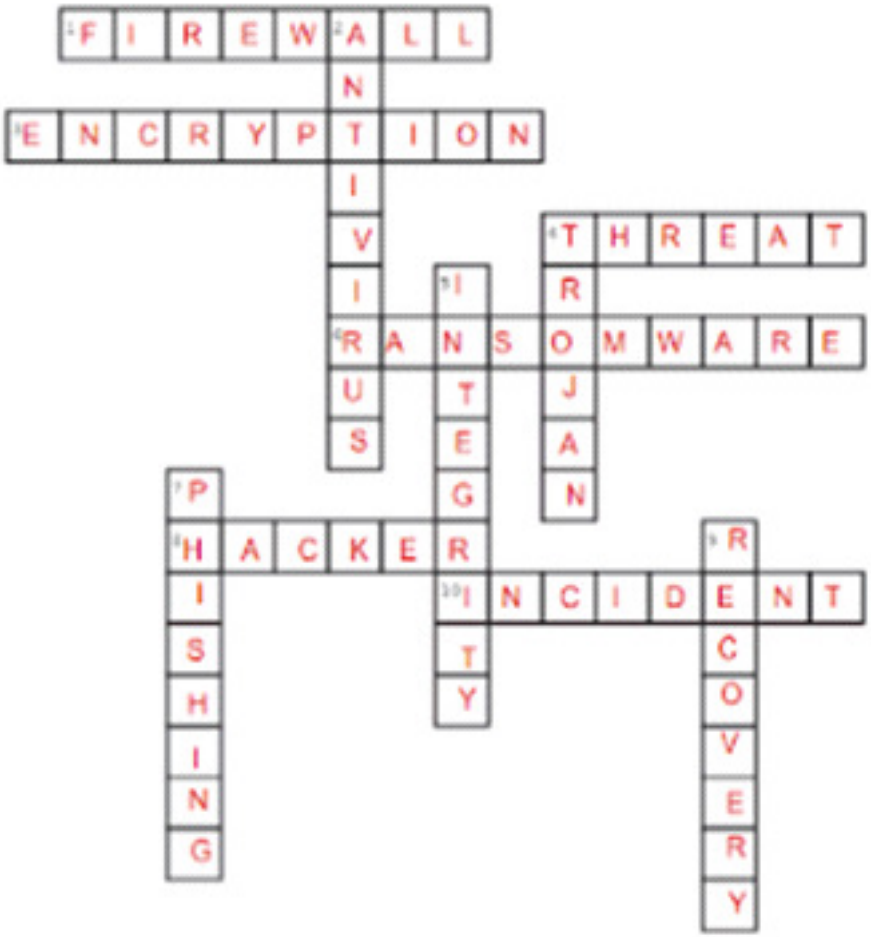
ISACA Bangalore Chapter - Certification Review Classes - 2022

Registration Link: https://www.meraevents.com/event/isaca-bangalore-chapter-certification-review-classes

ISACA Bangalore Chapter Telegram link: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA

Answers for Q4, 2021 Crossword

Crossword

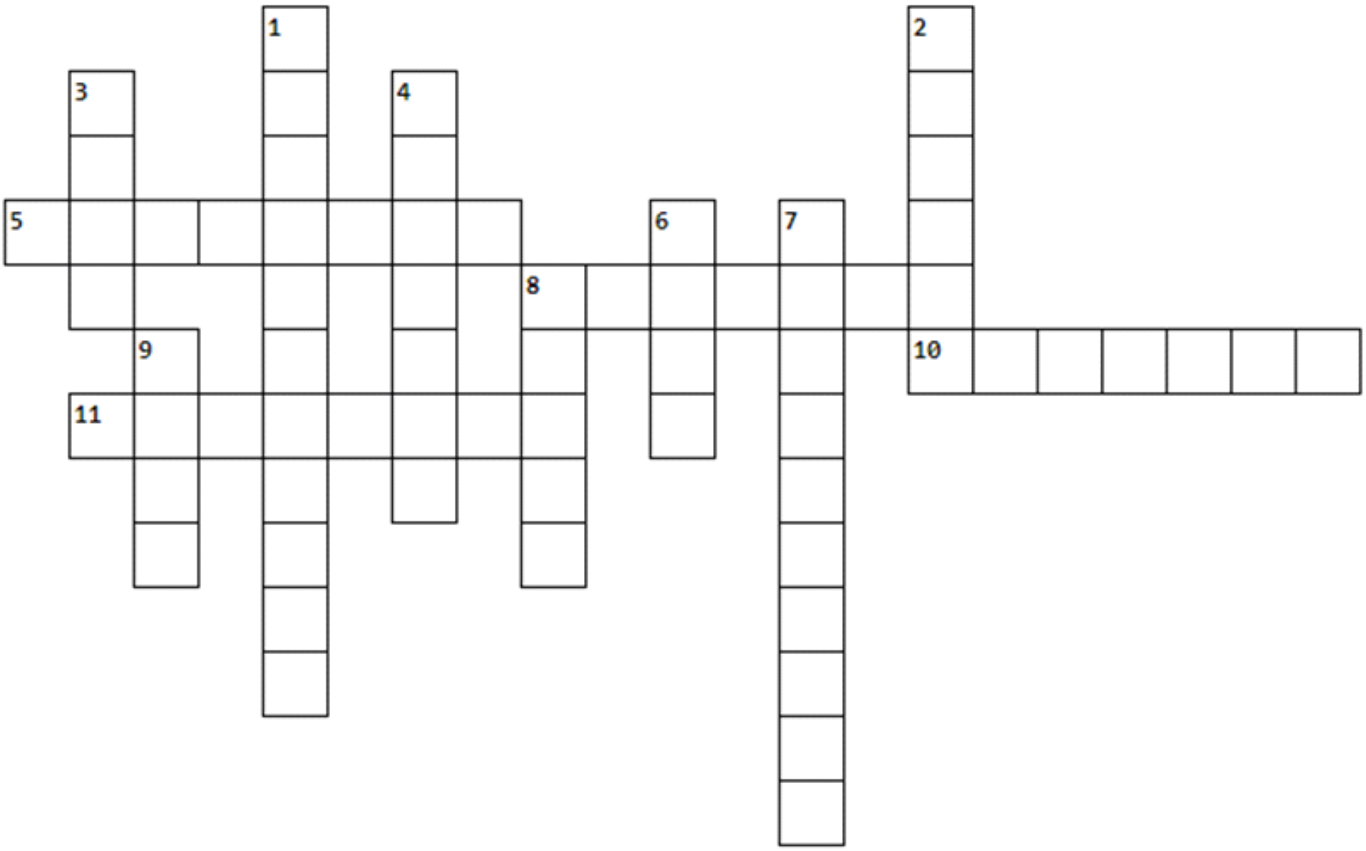


CROSSWORD INSTRUCTIONS:

- ISACA Bangalore chapter is excited to bring this crossword puzzle to our members
- We encourage our members to actively participate by filling this crossword in a paper (take a photo) / digital format and send your responses to **chapter@isacabangalore.org** via email before 28th February 2022
- While you are sending your response, please also mention your name, email address and ISACA ID
- Answers of the crossword will be published in the Q1, 2022 newsletter

Congrats!!!!! to Medhanand S (ISACA Bangalore Chapter Member) who has sent the correct answer.

CROSSWORD Q1, 2022



Across	Down
5. It is in Windows operating systems in the central set of settings and information required to rund the Windows Computer. 8. Malware that passes information about a computer user's activities to an external party. 10. It is a freeware protocol analyzer for Unix that can monitor network traffic on a wire. 11. The short name, usually meaningful in some way, associated with a particular computer user.	1. Obtaining services by using someone else's resources. 2. A TCP-based, application-layer, Internet Standard Protocol for remote login from one host to another. 3. Process in which network information is aggregated, sorted and correlated to detect suspicious activities. 4. These are used or shared by attackers before the software developer knows about the vulnerability. 6. The authorised use of personally owned mobile devices such as smartphones or tablets in the workplace. 7. It is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business 8. A Unix term for the interactive user interface with an operating system. 9. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

Crossword Created by Ganesan Ramani

ISACA Bangalore Chapter is happy to announce the Crossword contest. **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 June 03rd, 2022.

Terms & Conditions:

a. This contest is only for ISACA Bangalore Chapter members only. Other ISACA chapter members and non-members are not eligible to participate in the contest.
b. In case if there are only one or two winners from the total entries then the vouchers will be given only to them. If there are no winners then no gift vouchers will be given.
c. ISACA Bangalore Chapter Executive committee reserves all rights to drop / change this program, modify the gift vouchers value

Contributions to ISACA Bangalore Chapter Newsletter

Dear Members,

The Chapter Newsletter covers the updates on chapter events, technical articles and whitepapers related to the areas of emerging technologies, IT Governance, Audits and Cybersecurity. In this regard, we request our chapter members to send your technical articles and whitepapers to us.

You can send your articles / whitepapers to our chapter email address: chapter@isacabangalore.org

Regards,

Ganesan Ramani
Director - Newsletter, ISACA Bangalore Chapter

Support from ISACA Bangalore Chapter

ISACA Bangalore chapter contact details:

Website: https://engage.isaca.org/bangalorechapter/home

Chapter Office Address:
S-13, 531/A, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.

T: 8050030042 / 98865 08515 / 080-23377956

Email: chapter@isacabangalore.org

Telegram Channel: https://t.me/joinchat/AAAAAEt42QAUpWHucyNyJA

LinkedIN: https://www.linkedin.com/company/isacabc/

Facebook: https://www.facebook.com/ISACABC/

Book Post

If undelivered please return to :

ISACA
Bangalore Chapter

S-13, 531/A, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, Opp. St. Theresa's Hospital,
2nd Stage, Rajajinagar, Bangalore- 5600 10.
Ph. : 080-23377956 Email: chapter@isacabangalore.org

Printed @ Cauvery Ent. © 22128682

Chapter Reg No : 433/2002-2003