SECURE 'T' CAFE

Q1 2023

Menu

QUARTERLY NEWSLETTER

ISACA
Chennai Chapter

Cover page design: Copyright owned by ISACA Chennai Chapter. Created using Canva.

Vanakkam, Namaste 🙏

Welcome to ISACA Chennai Chapter's **Secure 'T' Café.** We take the pleasure of serving our quarterly newsletter on a new platter to all the security enthusiasts and our beloved members!!

Your interest fuels our energy!!!

What comes to your mind when you read the phrase 'Secure 'T' Cafe' – Security or Tea or Coffee?... to us, it was all three at once. We all are security professionals and mostly food lovers - thus was born the idea of collaborating Security along with Food, which is inevitable for a healthy and happy existence – but to be consumed carefully to satisfy our risk appetite!

So here is serving you a delectable menu of Security updates & Chapter news, Regulatory aspects on Information Technology / Systems Audit and many more….

Why wait? Read on and savour the flavors of our café!

SECURE STARTERS – Knowledge nuggets on Regulatory Updates

RBI - Empowering Digital Payment Ecosystem by Embedding Security

The Central Bank of any country is usually the driving force in the development of national payment systems. The Reserve Bank of India (RBI) being the Central Bank of India has been playing this developmental role and has taken several initiatives for safe, secure, sound, efficient, accessible, and authorized payment systems in the country.

RBI needs to manage the currency flow in the economy and to direct several Banks in various matters. The vast role of RBI shall be maintaining the price stability in the economy, improving the payment system by enhancing security to prevent illegal activities and providing the latest technology to the citizens to help them access the financial products with ease.

Enabling and enhancing digital payment through the Payment and Settlement Systems Act:

The initiatives taken by the Reserve Bank focused on technology-based solutions for the improvement of the payment and settlement system infrastructure, coupled with the introduction of new payment products by taking advantage of the technological advancements in Banks.

The RBI and RBI authorized Retail Payments Organization operate the following payment systems, viz., National Automated Clearing House (NACH), National Electronic Fund Transfer (NEFT), Real Time Gross Settlement System (RTGS), Immediate Payment System (IMPS), National Financial Switch (NFS), Bharat Bill Payment System, Payments through cards issued by Payment Networks, Payment Aggregators/Gateways, Mobile Banking Services, Prepaid Payment Instruments (PPIs), Unified Payments Interface (UPI), Digital Payment options for feature phone users (UPI 123Pay), National Electronic Toll Collection

(NETC), Aadhaar Enabled Payments System (AEPS), and Small value payments in offline mode.

RBI's continuous effort of enhancing and protecting the digital payment ecosystem:

Cybersecurity Framework:

In the race to adopt technology innovations, the Banking ecosystem and their service providers have increased their exposure to cyber incidents/attacks thereby underlining the urgent need to have a robust cyber security and resilience framework. The attack surface has expanded vastly. The RBI has provided guidelines on Cyber Security Framework vide *circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016*, to ensure adequate cybersecurity preparedness among Banks on a continuous basis. These guidelines were issued based on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (G. Gopalakrishna Committee) vide *Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011.*

RBI Cyber Security Framework addresses three core areas: (1) Establish Cyber Security Baseline and Resilience (2) Operate Cyber Security Operations Centre (C-SOC) and (3) Cyber Security Incident Reporting (CSIR).

This broadly covers, Cyber Security Organization, Cyber Security Strategy, Cyber Security Policy, Cyber Crisis Management Plan, Cyber Risk / Gap Assessment, Network and Database Security, Physical & Environmental Security, Third Party Risk Management, Cyber Security Awareness, Security Testing, Cyber Security Operation Centre, and Incident Response & Management.

Digital Payments Security Controls:

The RBI has given Master Direction *(RBI/2020-21/74 DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21) on February 18, 2021*, which provides necessary guidelines for the regulated entities (Commercial Banks, Small Finance Banks, Payments Banks, Card issuing NBFC) to set up a robust governance structure and implement common minimum standards of security controls for digital payments products and services.

The Master Direction was issued at a crucial time when the financial industry was in the mid of its rapid digital transformation due to the global pandemic disruptions and evolving security landscape. The guidelines issued are a technological and application-based framework that improves the digital payment environment for customers to securely embrace the evolving digitization of the financial industry.

This direction broadly covers, Governance and Management of Security Risks, Generic Security Controls, Application Security Life Cycle (ASLC), Authentication Framework, Fraud Risk Management, Reconciliation Mechanism, Customer Protection, Awareness and Grievance Redressal Mechanism related to Internet Banking Mobile Payments Application Security Controls and Card, Payments Security, and Special emphasis on following various Payment Card Security Standards as per Payment Card Industry (PCI).

Enhancing Security of Card Transactions:

To increase the security of card-based transactions, the RBI had directed all Banks on 15 January 2020 *(RBI/2019-20/142 DPSS.CO.PD No.1343/02.14.003/2019-20)* to extend the following facility to the cardholders where they can enable/disable their cards for various uses - online, physical, contactless domestically or internationally by themselves. Further, the Banks have also been asked to allow cardholders to modify transaction limits within the overall card limit for all types of transactions domestic and international at Point of Sale (PoS), ATMs, online transactions, and contactless transactions.

This broadly covers, the controls to be implemented by the Bank at the time of issuance and re-issuance of limits and channels for both domestic and international transactions, features available to the cardholders to turn off / turn on the transaction channels and modify the limits, alerts to be provided to the cardholder upon changes in any these controls.

The tokenization of storage of cardholder data:

Tokenization is the process of replacing original card details with an alternative code called a "token" which should be unique and provides an additional degree of protection for customer card details. Since the merchants could collect the cardholder information for processing the transaction, RBI issued guidelines restricting storage of cardholder data in the merchant app/system. The RBI has released multiple directions based on the scope of services provided by the regulated entities in the payment ecosystem, viz., *RBI/2018-19/103 DPSS.CO.PD No.1463/02.14.003/2018-19* on January 08, 2019 (Tokenization - Card transactions), *RBI/2021-22/92 CO.DPSS.POLC.No.S-469/02-14-003/2021-22* on August 25, 2021 (Tokenization - Card Transactions - Extending the Scope of Permitted Devices), *RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22* on September 07, 2021 (Tokenization - Card Transactions - Permitting Card-on-File Tokenization (CoFT) Services).

Tokenized cards can only be used with a specific merchant and customer. If there are any changes to the conditions under which the token was requested, it cannot be used to initiate a transaction. When a fraudster intercepts a regular card number from (for example) a poorly secured wireless network, they can try to use that card number anywhere, and merchants with weak anti-fraud defenses will accept it. When a fraudster obtains tokenized card data, it is useless to them. Merchants, or their service providers, can store tokens only if they are PCI DSS compliant.

This directive broadly covers, the scope of the token for the card number, the merchant, and the entity requesting the token (such as a payment processor), it also throws light on the following: every merchant should collect the customer's consent for tokenization through multi-factor authentication, customer should be provided with the option to delete/deactivate the token with merchant application, the merchant should only be able to view the issuing Bank, card network, and the last four digits associated with each tokenized card, etc..

The Regulator mandates a System Audit Report (SAR) by a third-party CERT-In empaneled agency to certify on the tokenized storage of card data, generation/degeneration of the tokens and management of the overall token lifecycle.

Storage of Payment System Data:

To have better control over the storage of payment data and the cardholder elements, the RBI wanted to restrict the storage of payment data elements within the Indian region and released a Master Direction (*RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018* on 6 April 2018) and further clarified on the subject through a FAQ (https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130)

This specified that crucial / sensitive details such as end-to-end transaction information, any details relating to payments or settlements that are sent, gathered, or processed as part of a payment message or instruction, customer information like name, etc., KYC details like Aadhaar numbers, etc., payment sensitive information like beneficiary and customer account information, login credentials like one-time passwords and PIN numbers must be protected in accordance with the guidelines.

The Regulator also mandated a System Audit Report (SAR) by a third-party CERT-In empaneled agency for all System Participants including their vendors.

Conclusion:

The Regulator has been continuously issuing guidelines to the Indian Banking industry and to the parties involved in Digital Payment Ecosystem to create a secure cyberspace to safeguard customer interest.

Information Security professionals play a key role in testing and implementing the controls effectively and in continuous monitoring for improvement which shall help the organizations in this industry to be compliant with the guidelines issued by the Regulator.

Taking the flavor from a CXO speech, “Information Security is like a traffic signal; the small stoppage/slowness caused because of incorporating process, and procedures only helps the organization to move (grow enormously) steady and stable.” (Mr. Prabhu, Co-founder, M2P Fintech).

- STARTERS TOASTED by Mr. Sundaravenkatraman

Chapter Events over a Cuppa 'T'

ISACA Chennai Chapter Professional Development Meetings (PDMs) conducted every 2nd Saturday are known for their unique topics and distinguished speakers – the trend continues in 2023 as well!!

The 1st PDM of the calendar year 2023 was held on January 14th, the day of Bhogi, which paves way for new beginnings, with the most happening of topics - PRIVACY!! Effective implementation of PIMS with ISO 27701 was presented by our Chapter member Mr. Ganesh Kandasamy. It was an extensive presentation chalking the journey of Privacy as a concept commencing from its evolution in 1604, as pronounced by Sir Edward Coke, up to the GDPR, which was a game changer in 2018. This was followed by a threadbare clause-wise analysis of ISO 27701:2019. The event was packed with 200+ members, virtually joining in. As the concept and content could not indeed be limited to the two-hour window, an extended session was scheduled on January 28, 2023, where

Mr. Ganesh Kandasamy enlightened the group with his insights on effective implementation of Privacy Information Management System (PIMS).

The February 11th PDM was yet another interesting session, with truly a topic of its kind where our Chapter member Mr. Ravikumar Ramachandran, elucidated on the various hats donned by the new age CISO, namely, the industry expectation, regulatory compliances, pain points and opportunities. The correlation between the four core principles of Agile Manifesto and the Role of CISO was especially incisive and highly informative.

March 2023 was indeed incredibly special for several reasons:

- The Founders Day, which was celebrated on March 4th, at Hotel Palmgrove, Chennai
- The 1st Physical PDM of 2023 was conducted on March 11th, at Hotel Maris Chennai.
- The Emerging Risk and Technology (ERT) Volunteer Group was formally introduced to the Chapter members
- The 1st News roundup was successfully presented by the News roundup group (sub-group of the ERT Volunteer group) and well received by the audience
- Gamified Cybersecurity strategy development workshop on March 18th, at the Deccan Plaza

The Founders Day program is one of ISACA Chennai Chapter's signature initiatives with handpicked topics of common interests, as it is a conclave of Chapter members along with their respective families. The august addressal by the Chapter President and Senior members was followed by the Guest talks - this time the 2 topics chosen were so diverse and delightful - one was Hidden Science in Art which explored the innate and incisive association between Astronomy, Astrology, Physical Science, and Mathematics by **Mrs. Archana Raghuram** and the other was on 'Sleep', its quality, quantity, timing and its utmost importance to wellness by **Mr. Arvind Ashok.** A treat to the mind was followed by a treat to the taste buds with a scrumptious dinner.

March 2023 PDM was a shocking revelation on the amount of digital invasion we have allowed onto our lives. Our Chapter member Mr. Anish Koshy, with his pristine thoughts and scientific analysis of cyber psychology and its dreadful impact on human behaviour, got the audience deeply ruminating about their current lifestyle. It was a perfect coincidence that such an awareness about digital detox and healthy living was disseminated in a physical meeting 😊

The gamified cybersecurity strategy simulation event on March 18th was attended by 24 delegates who were split across 6 teams. The game was made super exciting based on the Gartner-awarded cloud strategy simulation tool by Saras Venture. The delegates had almost a real-time experience building a cybersecurity strategy and aligning it with people, process and technology. The session commenced with a briefing on game-based learning and its advantages over traditional classroom learning and lasted for an engaging seven hours spread across four rounds, with all teams developing the right strategy to save money!!! Security can be Fun business too!!!!!

That was indeed a GULP not a SIP right 😉

- 'T' brewed by Ms. Sangeetha N

SIGNATURE SPECIAL – DIGITALLY YOURS

HOW BALANCED ARE WE, AS PROFESSIONALS?

It was a Monday morning. As usual, a pack of client calls had remained scheduled for our team playing the role of consultants. We were a team of five high-profile consultants supporting a global project. The call started on time and the consultants were sharing the status of the verticals they were supporting over the project. Conforming to the defined span of 10 minutes each, three consultants had completed their presentation in a span of 30 minutes and the fourth one followed suit. Half-way through his presentation, the participants felt a disruption, both in audition and presentation. The prolonged silence from that consultant was considered a technological disruption. To maintain time discipline, the fifth consultant started presenting and the discussion was closed after the fifth consultant completed his presentation.

Since, disruptions would normally be owing to poor internet connectivity or some technological issues with the system, and under such contexts the information would be shared over email, we did not pay much attention about the disruption in the presentation of the fourth consultant. But, on seeing the email that was received from the fourth consultant, the entire team was frozen with shock. The email ran as follows:

"…………..apologies for the disruption in my presentation. It was not owing to technological issues. But my voice got chocked all of a sudden and I am yet to have my voice resumed."

And we later understood that he got his voice resumed after three days. And the doctor who attended him on that score, had ascribed the cause to 'lack of work-life balance'.

Though initially I thought of writing an article on privacy based on legal conclusions, the one of the feedback the ERT team received upon its first presentation on 11th March, recommending for presenting information on emerging technologies and strategies, uncommon aspects and the like, this health incident triggered me to have this article centred on one of the most significant aspects – *work-life balance* - that would invariably remain neglected or provided with secondary, or in some cases, even least of importance, by many professionals such as CA, CISA etc.

There are many factors, as almost every one of us is aware of but invariably keep overlooking, that are the fulcra for the work-life imbalance. Considering the need to have this article concise, I would touch upon the factors only at a high level and avoid deep-dive.

Hurried Obsession:

We, as professionals, invariably keep ourselves in a state of hurry owing to several factors; commitment to clients, competing for business, knowledge enhancement, aligning with growing technology etc., are a few to quote. The beauty of this is that we suffer this sickness without even realizing that we are in sufferance. Hurriedly waking up, eating in a hurry (some even eating while driving or during conference calls), speeding through traffic, juggling four or five tasks at a time are the common symptoms of being in a state of hurry.

The increasingly rapid technological developments only add to this state and trigger our impatience when things are not achieved instantaneously. How agitated are you when the external network (internet) is slow? But have you ever realized how such an agitation weakens your biological network (brain, cells, nerves). I have known of people who are disappointed with God because their prayers are not answered instantly.

We tend to hurry up with life so much that we find ourselves running to detox centres and relaxation holidays only to load ourselves all over again. But detox and relaxation exercises will be of no help unless we bring the shift from within. Many of you would admit this fact; but might as well feel that it is a nice ideal, which is possible if we are living in an island and not in 21st century with expectation for instantaneous solutions, exponential rate of technology expansion etc. The fact is that even amidst such an environment, one can still be mindful of one's health. All that is required are simple practices.

(a) Spare at least 20 minutes for relaxation amidst the official or professional chores. Sit in your work chair (if you can afford to; else at any convenient spot) with eyes closed for 20 minutes in your day. Let these 20 minutes be totally yours as if the outside world does not exist for those 20 minutes. You will be surprised that your body would start identifying with the tension spots and keep healing.

(b) If your mind is overly hurried and confused, avoid your habitual walking. Instead, try to walk slowly and take each step consciously. This would enable you to get rid of your feverish mind of being hurried all the time and turn your awareness within.

(c) Whenever possible, maintain a relaxed breathing system. All you need to do is to focus your attention on breathing in and breathing out. This will turn your awareness within and in that the body starts healing.

Sleep deprivation:

Our circadian rhythm operates on a 24-hour cycle – same as a clock, hence the term biological clock. Biological clock is the term applied to the brain process which causes us to have 24-hour fluctuations in body temperature, hormone secretion and a host of other bodily activities.

It is this clock that gets confused when we stay up late. As a consequence, the circadian rhythm gets interrupted. When your rhythm gets interrupted, for example, if you experience several nights of sleep deprivation, it is thrown out of sync, causing many health issues such as mood swings, memory disorders, gastrointestinal disorders, cardiovascular diseases, and even reproductive risks. Our brain is programmed to act in different ways at different times of the day. So, systematize your routines. Try to establish a consistent schedule so that you go to sleep and wake up about the same time every day, even on holidays and off days. Once a biological clock gets attuned to a particular number of hours of sleep, it does not require more. Only the mind asks for it; the body does not.

Phase-out of human interaction:

You will agree that the level of in-person human interaction has been phasing out and replaced with virtual interaction. E-hugs and Emojis have become the mode of conveying love and affection; television, iPad or mobiles sing the lullabies for children; tech gadgets have replaced physical play fields for games; earlier, at least to reach an address we used to ask for routes and directions to people around. Now a Google map does this job for us.

This replacement from man to technology is making us loners. But we humans are not meant to live in isolation. And inherently too. This is why almost every one of us insisted for physical PDMs in ISACA, Chennai, post-corona. Living with machines and gadgets may seem convenient, and of course it is, but resultant deprivation of physical human interaction is likely to have both psychological and physiological impacts in due course.

So, try to remain a step away from technology to an affordable extent and be a part of physical interaction. Such interaction will keep you refreshed and healthy.

Lack of physical activity:

While so many people start off with exercise as a New Year resolution, seldom do they continue. Exercise in any form – be it physical exercise in a gymnasium or just jogging, walking, running, or playing some sport – can decrease stress hormone like cortisol and increase endorphins, your body's feel-good chemicals.

When you love exercising for good health, every cell in your body would feel good and desires to exercise a lot more. When you associate pain to exercise, with time you will find yourself back to the old days of inertia and every cell in the body associates pain to exercise.

So, make it a point that you spend some time for exercise on a regular basis, taking into consideration your present health condition, lifestyle etc. Life does give us several opportunities for exercise day in and day out. But how one makes use of those opportunities is what matters. For instance, you may choose staircase (I do mean flight of steps and not an escalator) than an elevator; avoid using vehicles to cover a distance, that can comfortably be covered by walk.

Eating habits:

The nature, type and quality of your food do contribute to your levels of health and energy. In this context, it is suggested to include vegetables and fruits as much as possible. This is because they have natural nutrients and nourish you with fibres, vitamins, and essentials minerals. Even if one is attached to non-vegetarian food, still it is advisable to include as many vegetables and fruits as possible in one's diet.

Foods may be broadly divided into alkaline and acidic types. While most of the vegetables and fruits fall into alkaline category, most of non-vegetarian foods fall into acidic category. Ideally, most of one's diet should consist of alkaline foods to balance PH level and maintain good health. When our body environment is more alkaline, the chances of diseases are less and when the body environment is more acidic the chances of diseases are much higher.

As important as avoiding junk foods, the composition of your food, the interval between two meals, your emotion while taking the meal, the awareness with which you take the meal etc., are important.

Conclusion:

You might wonder if it is possible to comply with the aforesaid tips at all times, in the prevailing technology-centric business environment. Remember, the only answer to this question is – **It is your choice.** If you prefer a wealthy professional life without compromising your health, you have no option than giving a serious thought to the tiny tips shared in this article.

We, as consultants, advocate risk assessment as the starting point for any business venture and maintain risk-based audit approach; but owing to professional appetite, we invariably overlook designing such assessments for our professional life or career. The negligence, which results in work-life imbalance, would normally show its heinous reflections, majorly from health perspective, only at much later stage when it may be irreversible.

It is never too late to get started in the journey of health. With due awareness and discipline, you will continue to achieve in your professional venture while maintaining good health.

Remember, Ctrl+Z or Ctrl+Alt+Del may work fine for your computer and definitely not possible in Health.

CURATED by our special chef Mr. Ganesh Kandasamy

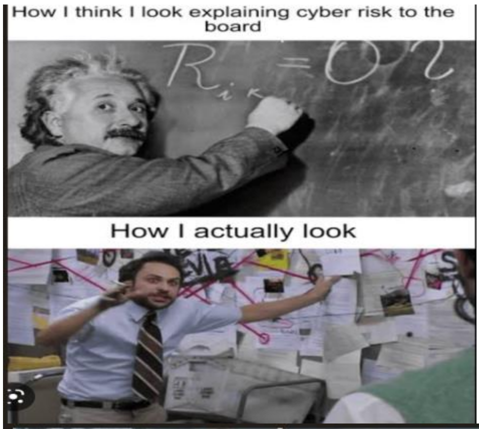
~~Milk~~ Handshake – Member Delight Series

Get to know of a Chapter member and his/her Journey with the ISACA Chennai Chapter - This time it is a Tete-a-Tete between our Chapter Members **Ms. Chitra Sathish** and **Ms. Sangeetha N** – Sometimes a '***HANDSHAKE'*** is all it takes to ***initiate a Communication Session.*** Grab your ear pods and listen in to the podcast below.

Access the Podcast

Note: *The views expressed here are the individual views of the respective members and are not representative of any organization or any certification bodies to which they are affiliated to.*

STRESS TEST – TRY DESSERTS – Laugh Out Loud n REFLECT TOO!!! 🤣



I.T. CONGRATULATING ME FOR NOT FALLING FOR THE PHISHING TEST
ME WHO DOESN'T READ EMAILS

Source: LinkedIn

Trust you all enjoyed our delicious spread @ Chennai Secure 'T' Café

PAM
~~PAAN~~ SUPARI and much more… coming up in our next edition…

Do drop by @ this space each quarter for more interesting ~~feeds~~ Menu

Give us your esteemed feedback @ https://forms.office.com/r/UUDXWW5LG9. It takes less than 2 minutes to complete the form.

Newsletter Editors: Sangeetha N and Sripathy Raagav K (ERT group members)

Newsletter Editorial Review: Jayasree Chandrasekaran and Vaidyanathan Chandramouli