Cybersecurity, IT Assurance & Governance Virtual Conference 2021
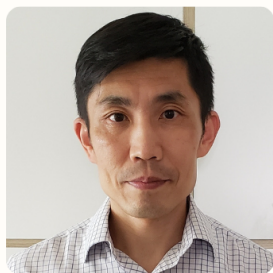
CIAG — CYBERSECURITY, IT ASSURANCE & GOVERNANCE

ISACA Malaysia Chapter

Working in Pandemic Situation
13th – 15th July 2021
Start at 09:00 AM to 14:00 PM

13 CPE ISACA MEMBERS

Supporting Organizations

ISACA Singapore Chapter
ISACA Bangkok Chapter
ISACA Indonesia Chapter
ISACA Macao Chapter
ISACA Manila Chapter
ISACA China Hong Kong Chapter

The Institute of Internal Auditors Malaysia

ACCA Think Ahead

CHARTERED ACCOUNTANTS AUSTRALIA + NEW ZEALAND

MICPA MALAYSIA

BCM Institute

HITB

CSA cloud security alliance®

After an unprecedented year caused by the COVID-19 pandemic, ISACA Malaysia is excited to announce the return of its Cybersecurity, IT Assurance & Governance (CIAG) Conference! As witnessed and experienced by many, past ISACA Malaysia's CIAG Conferences have featured some of the region's most esteemed subject matter experts, sharing their insights and knowledge on a wide range of cybersecurity, governance, IT risk management and assurance topics.

The return of CIAG conference this year comes with a refreshed format to cater to the new norm where it would be held virtually. It would also feature speakers not just from the Asian region but globally as well. This CIAG Virtual Conference will feature many points of views presented by our esteemed subject matter experts in various plenaries, panel and mini workshops / masterclasses covering various cybersecurity, governance, IT risk management and assurance topics.

The main conference on 13th and 14th July will feature the keynote address, plenary and panel discussion sessions, while 15th July conference day will be split into concurrent management and technical masterclasses covering the latest development on cybersecurity, IT governance, continuity management and assurance. These classes are designed to provide 'live' practical experiences and thoughts sharing by the speakers.

This year's CIAG will be fully electronic – in addition to the online program presentation, conference delegates can leverage on the conference virtual platform to stay in tune with the plenary speakers, conference schedules and provide feedback as well as accessing the presentation and sponsors materials. For full CIAG details, visit www.isaca.org.my

Virtual Conference Day 1: 13th July 2021

Time	Session
09:00 – 09:10	**Opening Remarks – Organizing Committee Chairperson:** *Jasmine Goh*
09:10 – 09:50	**Keynote:** **Emerging Technology in 2021 and Beyond** *David Samuelson* *ISACA CEO* Join ISACA CEO David Samuelson to discuss our latest emerging tech research and the implications it has now and in the future of your roles. He will discuss ISACA's current strategy that includes digital-first initiatives, a focus on global impact, creating an enterprise ecosystem, and developing our next generation workforce. Time will be allotted for conversation and questions.
09:50 – 10:05	**Break**
10:05 – 11:00	**Plenary Session:** **Ransomware: The Second Pandemic** *Jaco Benadie* *Executive Director & Head of Cyber, KPMG in Malaysia* Ransomware may have started back in 1989 but first gained global notoriety as a result of the WannaCry attack in 2017. This campaign was unprecedented in scale, with an estimated 200,000 computers across 150 countries infected. Some unfortunate organizations spent in excess of US$100M to recover from this infection. The COVID-19 spread prevention lockdown orders resulted in a significant shift towards remote working with a rise in ransomware incidents. Vulnerabilities in people, process and technology controls, due to the move to remote working over this period have presented huge opportunities for cyber criminals.
11:00 – 11:15	**Break**
11:15 – 12:10	**Plenary Session:** **Present and Future Cybersecurity for Companies** *Alvin Rodrigues* *Field Chief Security Officer, APAC, Infoblox* Covid is a catalyst that accelerated the execution of digital transformation initiatives for many companies. In this presentation, we will discuss some of these initiatives and the role of cybersecurity. We will also review how cybersecurity has evolved over the last 14 months, what companies can do to secure remote work, and how cybersecurity needs to adapt as businesses continue to change in the present and post-pandemic. We will also discuss a framework that shows a symbiotic relationship between business, the company's digital footprint and cybersecurity. And the role of DDI to provide visibility, automation, and support security.
12:10 – 12:25	**Break**

12:25 – 13:20

Panel Discussion: The Opportunity of the "New Norm"

Chair: *Nickson Choo, Deputy Director, Bank Negara Malaysia*

Panelist:
- *Nazlee Binti Abdul Hamid, Group Chief Audit Executive, Maybank*
- *Leong Sow Yoke, Retired Group Chief Internal Auditor*
- *Marcus Or, Technology Risk and Compliance Manager, Crypto.com*
- *Neha Malhotra, VP, Cybersecurity Program Manager, Credit Suisse*

It has been 17 months (and counting) since we first encountered the current unprecedented pandemic situation, which brought massive disruptions to our lives and economic. However, this has also created opportunities for us to change the way we work, how to interact with people, how technology enabled and how to sustain our wellbeing in order to continue with our daily lives.

Join us in this panel discussion to get insights from leaders of different industries and experience on:
- The opportunities and challenges of digitalization transformation from areas such as e-services, cloud strategy, and data privacy
- How to handle and adopt the policy change, perform audit engagements/reviews, oversee & manage risk arising from the different way of work and digitalization
- The rise of cybersecurity incidents such as ransomware attacks, data leakages on third parties and other various cybersecurity risks to be mindful of

13:20 – 14:00 | **Virtual Booth Visit**

End of Day 1

Virtual Conference Day 2: 14ᵗʰ July 2021

09:00 – 09:05 | **Welcome Back / Recap Message – Organizing Committee Chairperson:** *Jasmine Goh*

09:05 – 10:00

Plenary Session: Resiliency in Da House

Bruno Soares CISA, CGEIT, CRISC, PMP, COBIT2019
Executive Advisor, IDC Portugal

The post-COVID "New Normal" will not have much of normality and VUCA world is here to stay.

Businesses will require operational resiliency to respond to the internal challenges, but risks will come much more from the ecosystem, forcing organizations to ensure supply chain trust, work-from-home (WFH) seamless experiences or to stay connected and aligned with the customers and consumers' needs. In the search for operating excellence, Information and Technology governance and management will have to be well aligned with Digital Engineering.

Will the next COBIT version have to change its name to COBOIT to address the OT/IT convergence challenges and keep resiliency in da house?

10:00 – 10:15 | **Break**

10:15 – 11:10

Plenary Session: IT Auditing in the New Normal

Tichaona Zororo, CIA, CISA, CISM, CRMA, CRISC, CDPSE, CGEIT, COBIT Certified Assessor
Digital Transformation and Innovation Advisory Executive with EGIT, Enterprise Governance of IT (Pty) Ltd

To be announced. Find out on the latest details in the CIAG2021 site: www.isaca.org.my

11:10 – 11:25 | **Break**

11:25 – 12:20

Plenary Session: **Building a Privacy-Aware Framework**

Henry Ng CISA, CISSP, ISSAP, CDPSE, CCSK, Microsoft Azure AZ-900
Director and Principal Consultant of KRIS Consultancy

Cybersecurity is becoming a daunting task for many security professionals as more and more security vulnerabilities and attacks are uprising. With an increasing number of data breaches and data extortion cases, managing data privacy has become a board-level priority for many organizations. Enterprises are striving to implement appropriate controls to protect and manage an individual's privacy throughout the life cycle of personal and sensitive data. They are looking for an established privacy framework so that enterprises can apply privacy controls to all aspects of business activities.

Henry will introduce a few prominent privacy frameworks including NIST Privacy Framework and ISO 27701 Privacy Management System, and explain how enterprises can apply these frameworks to implement an organization-wide privacy framework; and cover some cybersecurity models which can also be leveraged to build a privacy-aware enterprise framework.

12:20 – 12:35   **Break**

12:35 – 13:30

Plenary Session: **COVID-19 Pandemic: Strategic Shift in Managing Business Continuity**

Dr Goh Moh Heng
President, BCM Institute
Managing Director, GMH Continuity Architects

The changes and adaption by the businesses to manage the COVID-19 threat had resulted in business continuity management (BCM) practice and processes undergoing a major strategic realignment to this changing environment. Dr Goh will share the strategic BCM shift that professionals will have to respond and adapt to these changes as organizations are moving toward a virtual operation, redesigning physical operations, refining security protocol, reviewing policies and compliance requirements, realigning business continuity protocols, and driving toward business and operational resiliency.

13:30 – 14:00   **Virtual Booth Visit**

End of Day 2

Virtual Conference Day 3: 15th July 2021

09:00 – 09:10   **Welcome Back / Recap Message – Organizing Committee Chairperson:** *Jasmine Goh*

09:10 – 10:25

Technical Masterclass: **Sustainable Cybersecurity Strategy for the New Normal**

David Rajoo CISM, CISSP, CCSP, ZTX-I, CCSK
Country SE Head, Cybersecurity Engineering, Palo Alto Networks Malaysia

We will introduce the cybersecurity concept of ZeroTrust and the role it plays in securing digital transformations, especially in the context of the new normal.

Key Takeaways:
- Understand how Zerotrust can be done sustainably and pragmatically
- Adopting the ZeroTrust strategy can increase the efficacy of security solutions while at the same time having a positive impact in ROI and TCO

Management Masterclass: **Managing Cyber Risk in a Post-COVID-19 World – Lessons Learnt from Latest Breaches and Incidents**

Gan Kok Tin CISA, CISM, CCA
Partner, PwC Hong Kong

Clarence Chan CISM, CDPSE, CIPT, CPA
Executive Director, Digital Trust & Cybersecurity, PwC Malaysia

Over the last 12 months, we saw a spike in cybersecurity incidents with significant impact on organizations already dealing with the challenges posed by the pandemic such as COVID-19 themed phishing and spear-phishing attacks; perpetrators exploiting the popularity of COVID-19 related news and headlines; and ransomware attacks compromising remote services (or work from home set-ups).

We will cover key trends and highlights from PwC Digital Trust Insights Survey 2021 – a Malaysian perspective; how the trends correlate to actual attacks observed on the global landscape; review the lessons learnt from latest high-profile attacks.

10:25 – 10:40   **Break**

| 10:40 – 11:55 | **Technical Masterclass:** Step Up Your Game. Be Ransomware Ready with a Data Resilience Recovery Plan | **Management Masterclass:** How to Anchor Trust in an Increasingly Connected World |

Sathish Murthy, Director of Systems Engineering for Cohesity ASEAN / India region

Welland Chu, Business Development Director, APAC, Thales

Ransomware is the fastest-growing type of cybercrime. Analysts predict ransomware will attack a business every 11 seconds by the end of 2021. And every time a cybercriminal succeeds, the organization attacked is damaged — financially and often reputationally. To protect your organization from the crippling effects of a ransomware attack — you need to have a Beyond Backup Data Resilience Recovery plan.

Key Takeaways:
- How you can prevent your backup solution from becoming a ransomware target
- Why taking a multi-layered approach to data protection is the best way to safeguard your backup data against ransomware
- And if the worst happens, how quickly can you recover to reduce downtime and data loss

Over the past decade, the cyber security incidents that have caused devastating damages have been attributed to something called "supply-chain attack". These hacks include Stuxnet (first uncovered in 2010), Target (2013), SolarWinds (2020). Anatomy of these attacks indicate the hackers were targeting wider and lower in the platform stack. The attacks were successful by abusing the trust the users have on their hardware and software.

As our world is becoming more connected, we must rethink our strategy of establishing and assuring trust. Join this 1-hour session and learn how we may leverage the Hardware Security Modules (HSMs) technology to anchor trust in an increasingly connected world.

| 11:55 – 12:10 | **Break** |

| 12:10 – 13:25 | **Technical Masterclass:** Best Practices for Securing Robotic Process Automation (RPA) | **Management Masterclass:** Managing Data Breach and Cyber Fraud Post COVID-19 |

Dr Suresh Ramasamy CISM, CISSP, CDPSE, IAPP Chief Research Officer at Center for Advanced Computing and Telecommunications

Raymon Ram CFE, CAMS, ISO 37001 ABMS Lead Auditor, Masters (Economic Crime Management), Certificate In Corporate Governance (Basel Institute on Governance)

RPA (Robotic Process Automation) is a powerful technology that streamlines and standardizes process-related tasks. The technology is rapidly gaining popularity and is increasingly seen as a key element for digital transformation. When properly applied, RPA can increase productivity and data quality and ensure better compliance with laws and regulations. Employees can then focus on more strategic, more interesting work.

This session will discuss on the RPA context of best practices for RPA Security.

Key Takeaways:
- Introduction to RPA Security
- Challenges of RPA Security
- Mitigation of Security Risk in RPA

Fraudsters are continuously looking to exploit the weakest link within IT infrastructures. The current remote working arrangements due to the COVID-19 Pandemic has given them an upper hand to exploit both system vulnerability and human gullibility. This session will discuss the anatomy of cyber-attacks and current threat vectors which individuals and organizations need to take into consideration when setting up controls and designing cyber security preparedness training for persons associated to the organization.

Key Takeaways:
- Latest data breach and cyber fraud threat vectors
- System vulnerability and human gullibility as primary facets to cyber attacks
- Developing cyber-security awareness amongst persons associated to the organization

| 13:25 – 14:00 | **Lucky Draw & Closing Remark** |

End of Day 3

About ISACA Malaysia

ISACA Malaysia is the local chapter affiliate of an international body of information governance professionals known as ISACA (previously known as Information Systems Audit and Control Association, ISACA goes by its acronym only to reflect the broad range of IT governance professionals it serves) and has over 1,200 local members in Malaysia. The local chapter's objective is to promote research, standards, competencies and practices for effective governance, controls and assurance of information, systems and technology.

As a not-for-profit organization, the organizing committee of this Conference are volunteers. Proceeds from this conference are for the benefit of the chapter's activities. For more information, go to: www.isaca.org/malaysia

CYBERSECURITY, IT ASSURANCE & GOVERNANCE VIRTUAL CONFERENCE 2021
WORKING IN PANDEMIC SITUATION
13th – 15th JULY 2021 [9.00AM – 2.00PM]

REGISTRATION FORM

Contact Person Details

Organization Name	
Address	
Name	Designation
Email	Tel.

Delegate Details

No	Delegate Name │Designation	ISACA Membership #	Supporting Org. & Membership #
1			
2			
3			
4			

Fee (For Each Delegate)

Early-Bird Fee (by 27th June)	Normal Fee (after 27th June)		
RM 1,080	RM 1,280	- Normal Delegate	
RM 980	RM 1,180	- Supporting Organization Member	
RM 780	RM 980	- ISACA Member	

For special package of 5 or more delegates from the same organization, contact us at officeadmin@isaca.org.my or +6017-2196225 (Mr. Jayaseelan)

Payment Details

Please email the payment details / remittance advice for our records before places are confirmed.

	Direct Bank-In made (Ringgit Only) Bank Information: Malayan Banking Berhad │ Account No.: 512231822725 *Bank in slip / confirmation MUST be emailed to officeadmin@isaca.org.my with cover note stating organization name / delegate details.*

	Enclosed is a cheque / bank draft payable to **INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION**		
	Cheque / Bank Draft No.		
	Bank	Amount (RM)	

Important Information

As good practice, ISACA Malaysia Chapter is informing you that your personal data will be processed, retained and used by ISACA Malaysia Chapter in relation to this training event. Your personal data may also be retained and used by ISACA Malaysia Chapter to market and promote training events conducted by ISACA Malaysia Chapter.

ISACA Malaysia Chapter reserves the right to make changes / amendments to the program should unavoidable circumstances arise.

Registration will only be confirmed upon receipt of registration e-form, followed by payment. Payment has to be made before the Virtual Conference to guarantee the delegate's place.

A refund minus a service charge of 10% will be levied for cancellations received in *WRITING by 1 July 2021*. No refund will be made for request after this date. Substitutions are allowed for a registered delegate.

Note: This is an editable PDF.