Your Guide to Planning & Responding to a Cyber Attack

Waldorf Astoria The Palm Dubai

16th October

ISACA
Trust in, and value from, information systems
UAE Chapter

CYBER MANAGEMENT ALLIANCE

ISAFE 2016
10 years of success
INFORMATION • SECURITY
AUDIT • FORENSICS
• EMERGING TECHNOLOGIES

1 Day Strategy Session

For Mid - Senior Executives

CYBER INCIDENT PLANNING & RESPONSE

Intensive Workshops

Interactive

Immersive Learning

Can your business swiftly discover and then recover from a cyber attack? Most companies are unable to discover cyber criminals for an average of 200 days and many enterprises fall short after they discover their confidential and sensitive data has been breached.

To survive as a business you must be able to lower your time to discovery and time to respond. Furthermore, the tactical and strategic planning required to deal with complex and dynamic cyber threat actors requires a different and efficient mind set.

Interactive Sessions   SYLLABUS   Immersive Learning

- The "golden hour" and why it's critical to managing an incident.
- Effective incident planning & response strategies to tackle all types of simple and complex cyber attacks.
- Strategies to design an early warning system to lower discovery time from months to days and actionable strategies, response plans & checklists to use today.
- Understand how to define and baseline "Normal" within your organisation.
- Understand the business context on the technologies that underpin cyber incident response.
- Stop up to 90% of cyber attackers in their tracks .
- Strategies and guidance on how to build an effective cyber response team.
- Threat Intelligence for executives and how you can use it to defend your business.

● **971 50 8679196**   ● **isafe16@isacauae.org**   ● **www.isacauae.org**

TRAINER AMAR SINGH

- UK Government GCHQ Certified Trainer and creator of APMG & GCHQ Certified course CSPE (Cyber Security & Privacy Essentials)
- Creator and trainer of business focused Cyber Incident Planning & Response Course for middle to senior executives. (CIPR)
- Experienced cyber, information security & data privacy practitioner. Senior C Level Executive, Global Chief Information Security Officer, Expert in Information Risk Management.
- Mentor & Trusted Advisor to FTSE 100 Firms, Start-ups & Incubator Funds.
- Author, writer, industry speaker & presenter.

Who is this course for?

No pre-requisites and is tailored for both technical and non-technical individuals.

- CIO, CTO & IT Directors.
- Project Managers & BCP Managers
- IT Managers & Service Managers
- Mid to Senior IT Administrator & Network Managers
- Change & Incident Managers
- Head of Audit & Senior Auditors,
- Information Security Managers & Head of Security
- Legal & compliance

Download the CIPR Mind Map Free

Go to http://hubs.ly/H01VWvt0 or Click on the image to download your free copy

CYBER INCIDENT RESPONSE TRAINING
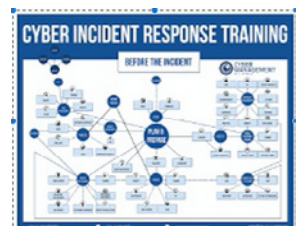
"... The Cyber Security landscape is constantly changing, and experts on the ground like Amar are highlighting the realities, not merely the theory, of dealing with these threats…"

Vijay Rathour,
Vice President at Stroz Friedberg Limited

Nour H. Kassassir
Vice President, Parsons

Nour Kassassir is the Vice President and International Director of Information and Communications Technology (ICT) for Parsons. Nour focuses primarily on the Middle East and Africa (MEA) region, is responsible for all ICT planning, design, execution and operations for all of Parsons employees across the MEA Region. Mr. Kassassir is an ICT Executive Management Professional with 30+ years of extensive & solid experience in IT Service Delivery & Management in diverse industries including: Automotive, Architecture, Engineering, Construction, and Oil & Gas in the U.S., Middle East, Europe, and Asia regions, including the following countries: UAE, Qatar, Saudi, Oman, Bahrain, Jordan, Indonesia, Italy, & U.K. Nour's experience includes the transformation of organizations & propelling them to new heights by applying big-picture vision, finding innovative solutions & astutely directing the creation and execution of short- & long-term strategies. He is familiar with building top-performing international operations from the ground up in difficult conditions through tenacity, intuition & multicultural relationship building. Nour successfully recruits, leads & inspires teams that harness the power of advanced technology to achieve critical business & financial objectives.

Mr. Kassassir holds a bachelor's degree in civil engineering and a master's of science degree in structural and geotechnical engineering from Wayne State University in Detroit, Michigan. Nour is a licensed professional engineer (P.E.) in the state of Michigan, USA. He is a certified project management professional (PMP®) from the Project Management Institute and holds an Information Technology Infrastructure Library (ITIL) Foundation Certification.

Mr. Kassassir is a member of Bentley's EMEA Construction Advisory Council. Nour also received the 2016 CIO of the year award from ISACA-UAE Chapter.

In his 30+ years in the ICT industry, he led and participated in mega projects such as the planning, design and construction of General Motors' 12000-employees world headquarters in Detroit-Michigan, U.S.A. Through his 17 year-tenure with Parsons, Mr. Kassassir supported Parsons MEA's organic business growth wherein Parsons staff has increased from 1000+ to 5500+ within the MEA Region.

Steve Tonella
Business Leader, Watchful

Steve Tonella with proven success in exceeding revenue targets, building & scaling local/global sales organizations in high growth and turnaround business environments. He brings 15+ years of Business Leadership experience which includes companies such as Cisco, Nimsoft (Acquired by CA), McAfee (Acquired by Intel) and Jive Software (Sequoia Backed). Steve has built up cross functional sales teams in the Americas, EMEA, Asia Pacific and speaks Spanish & Italian. Currently Steve is the COO of Watchful Software, a data security software company that provides advanced persistent security solutions that keep sensitive information safe from security breaches resulting from accidental or malicious disclosure. Watchful was formed to protect an organization's most critical asset after its people – its information.

Syed Wajat Ali
Head of Telecoms and IT Audit, du

Syed Wajahat Ali is responsible for providing technical assurance across the entire IT Applications and Infrastructure, Network Infrastructure and Platforms, Information Security functions and supporting business processes across du.

Prior to joining du, Syed worked in Internal Audit at several companies, including Mobily, Royal Bank of Scotland, Bank of New York Mellon & as a Client Manager at the British Standards Institute.

Syed received a Master's in Information Management & Finance from University of Westminster in 1999. He is currently working on a varying set of technologies including Mobile, Smart City, IoT, M2M along with evolving telecoms infrastructure and applications.

Manish Tiwari
Chief Information Security Officer, Microsoft India

A result driven Cyber Security professional, with notable and pioneering success in various IT security initiatives with a total of 28 years working experience and more than 22 years of relevant experience in IT & IT security.
I have worked in all aspects of Information Security namely policy framework, security audits, testing of products, implementation of solutions, Cyber Forensics and Risk Management etc., thus resulting in a strong foundation for Information Security management. Particularly proficient in coordinating and directing all phases of Project based efforts, whilst managing, motivating, guiding and mentoring teams.

After working for many years in CERT-Navy, took over as Director of CERT-Navy and Information Warfare in Indian Navy (responsible for all Cyber related activities in Navy) in 2008 and oversaw the growth of the IT security organization from 9 personnel to over 80 personnel. This involved talent recruiting, induction and training of suitable and talented personnel in cyber security core competencies. The responsibilities also included evolving a long term Secure IT strategy for the Navy.

In the last two years, I have had the opportunity to help execute critical security related milestones in the UID Aadhaar project and now in Microsoft India, set up a Cyber Security Team, as well as a Cyber Security Engagement Center.

David A. Cass
Chief Information Security Officer
IBM Cloud & SaaS Operational Services

Mr. Cass is the Chief Information Security Officer for IBM. He has global responsibility for all aspects of security practices, processes, and policies across the IBM Cloud & SaaS business unit. Mr. Cass serves as a regulatory SME and an Executive Steering committee member for IBM's International Banking Customers. David is an active contributor to the FS-ISAC on Cloud Compliance and Security for financial services firms, and works closely with U.S., and International Regulators.

Previously Mr. Cass served as the SVP & Chief Information Security Officer for Elsevier. Where he lead an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier. He also served as the HIPAA officer for Elsevier. David has over 4.5 years of experience running a regulated enterprise in the cloud.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase, and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is also a frequent speaker at high profile industry conferences, and serves on the Board of Directors for PixarBio Corporation.

Dhiraj Sasidharan
Director Compliance & I.T. Risk Management,
Jumeirah Group

Dhiraj is a seasoned IT professional who has more than 15 years of experience in Information Security. He works for a regional hospitality group and is responsible for their IT Compliance and Risk management initiatives and implementations. He is part of the larger Information Security function, providing input to IS strategy and executing tactical plans across the group. He has previously held Information Security roles at a large regional payment card processor and banking institution, which allowed him to experience the challenges, pitfalls and eventual rewards as companies went about their compliance implementations, securing network, infrastructure and application environments, preparing and executing incident response and recovery mechanisms and negotiating with stakeholders across Business and IT units.

K. K. Mookhey
Principal Consultant, NII Consulting

KK is one of the pioneers of information security in India. Having begun his firm as a one-man show in 2001, it has now grown to a team of over 250 consultants spread across multiple locations in India and the Middle East. He is a trusted consultant and trainer to organizations all across the globe on various aspects of information security. He is well-versed with the security challenges of various industry verticals, and also with international standards and frameworks such as ISO 27001, PCI DSS, COBIT, HIPAA, etc.

He is the author of two books (on Linux Security and on the Metasploit Framework) and of numerous articles on information security. He was the first security researcher from India to present at Blackhat in 2004 (on 'Detection and Evasion of Web Application Attacks') and since then has spoken at numerous conferences such as Interop, OWASP, NullCon, etc.

He is currently overseeing the research activities within NII focused on use of big data in security, building various automation solutions, and security impact of the Internet of Things.

George Eapen
Chief Information Security Officer
GE

George Eapen is Chief Information Security Officer (CISO) for GE in Middle East, North Africa & Turkey In his role, George is responsible for defining Cyber Security strategy for Enterprise IT & OT for the region and provide strategic leadership to IT Security related projects & initiatives for all GE businesses in the region. George is also responsible for protecting GE critical assets in a growing region which spans 18 countries and 7000 work force George joined GE in 2006 with GE Healthcare in India and has since held roles of increasing responsibilities and progressed to his most recent role as Chief Information Security Officer for MENAT.

During his tenure with GE, George worked in multiple domains (Product Life cycle management, ERP, Infrasrture, Supply Chain & Commercial IT) and multiple businesses (GE Healthcare,

GE Appliances, GE Capital, GE O&G, GE Aviation and GE Corporate) George is a graduate of GE IT leadership program (ITLP), GE Six Sigma Black Belt program and graduate of GE Executive leadership program (CAS)

C.Pandu Rangan
Senior Professor, IIT, Madras, India

Prof C.Pandu rangan obtained his Masters in mathematics from madras university and PhD from Indian institute of Science, Bangalore, IISc, India. He joined the faculty of IIT, Madras in 1982 and joined the rank of professors in 1995. he chaired the dept from 1998 to 2001 when the department witnessed multifold growth in research and infrastructure. He held visiting positions and chair professorship in various universities and industries in USA, Canada, Japan, Germany, Korea, Hong kong, taiwan, Dubai, Australia, and Switzerland. He is honored as FELLOW of Indian national Academy of Engg from 2006. He has served as Director in several boards. He is in the editorial board of LNCS, Springer Verlag, Germany.

He was a member of founding Team for IIT, Hyderabad and First Head of Indian Statistical Institute, Chennai. He has over 200 research publications to his credit in various reputed journals and conferences, covering different aspects of Algorithms and Cryptology.

CYBER RESILIENCY

CONFERENCE AGENDA

DAY 1: 17th Oct 2016

8:30am to 9:15am	**Delegate Registration & Networking**
9:15am to 9:20am	**Opening of the Conference – National Anthem**
9:20am to 9:30am	**Welcome address by Hari Prasad Chede, President ISACA UAE Chapter**
9:30am to 10:00am	**Key note Address**

10:00am to 10:30am   **Building a Resilient Critical Information Infrastructure & Effective IT Risk Management –** by Manish Tiwari, CISO, Microsoft India

Information security has become a priority concern for enterprises and public sector organizations alike. Insiders, hacktivists, criminal gangs and nation states are perpetrating cyber-attacks with increasing scale, sophistication and impact. In the face of these challenges, security leaders are reorienting their approach. They are establishing both the capacity to withstand attacks and a much greater ability to detect, contain and rapidly recover from disruptions. This transformation in security strategy marks the shift towards building cyber resilience.

The session will highlight as to how technical vulnerability can be reduced and how protective, detective, containment and recovery controls act in concert to identify compromised systems and minimize the impact of an attack. Since technologies and approaches that have provided the foundations for information security to date are now proving inadequate in the face of more sophisticated threats, game-changing technologies can turn the balance against the attacker. These include virtualization on devices, private and public clouds, the use of sandboxes for protected environments, trusted platform modules on general devices and use of machine learning and data analytics. Used in combination, these new technologies hold great promise for enhanced levels of resilience.

10:30am to 11:00am   **Converged Security** - by Nour H. Kassassir, Vice President, Parsons

Advances in technology, along with the capacity enhancement of IPv6 are enabling new concepts such as the IoT, IIoT and IoE. These new capabilities have fuelled the rapid expansion of Smart Infrastructure, dramatically improving efficiency and effectiveness, but create new security vulnerabilities. Physical systems, including security systems are dependent on information systems and vice versa, creating new levels of interdependence and new levels of risk. The convergence of physical and information systems necessitates a new way of thinking regarding security, CONVERGED SECURITY.

CONVERGED SECURITY Is the strategic and collaborative integration of an organization's physical and cyber security resources (IT, OT and Physical Assets) to achieve enterprise-wide benefits of enhanced risk mitigation, mutual protection, increased efficiency, reduced cost, full visibility into the enterprise security state, coordinated planning, budgeting and response. Such integration enables an organization to establish and manage a single, consolidated repository for all authentication credentials and to have a centralized means of setting access privileges for both physical and logical resources. It also addresses the increasingly exploited gap created between physical and cyber security, providing consolidated security monitoring, mitigation, response and recovery.

CYBER RESILIENCY

CONFERENCE AGENDA

DAY 1: 17th Oct 2016

11:00am to 11:30am	Networking Break with Tea/Coffee

11:30am to 12:00pm — **Auditing the Internet of Things (IoT) & Smart Cities**
– by Syed Wajat Ali,Head of Telecoms and IT Audit, du

- Introduction
- Background around Telecoms Auditing
- IoT/Smart Cities Technologies Overview
- Technical Challenges within the IoT/Smart Cities
- Embedding Audit and Control Framework
- Security & Future of IoT/Smart Cities

12:00pm to 12:30pm — **How to implement effective Enterprise Cyber Security**
- by George Eapen, CISO, General Electric (GE), MENAT

Many organizations realize that it is in their best interest to implement an existing information security standard rather than developing a customized information security framework. The most dominant information security standards today are ISO/IEC 27001 and NIST 800-53 standards. This talks will focus on the strengths and weakness of both standards and ways to pick the right standards for your organization.

- Introduction
- What are the top Cyber Risks in an Enterprise
- How do you develop partnerships with other functions to mitigate Cyber risks such as Employee experience
- BYOD and Security challenges Emerging Cyber risks- IT Vs OT

12:30pm to 13:00pm — **Data Security Compliance, Protection & Resilience**
– by Steve Tonella, Business leader, Watchful
A summary view of the environment, challenges and considerations facing organizations today to protect their most important data & information assets.

13:00pm to 14:00pm — **Lunch Break**

14:00pm to 14:30pm — **Cyber Security for Information Assurance**
-by C.Pandu Rangan, Senior Professor, Department of Computer science IIT, Madras. India.

Information Assurance is concerned with maintaining integrity/confidentiality/ availability of information that is stored or transmitted, in spite of attacks, accidents, technology or operational failures. Cyber security is at the core of defining appropriate defense mechanisms, such as policies, procedures, protocols, algorithms and hardware to achieve information assurance. Our talk focuses on the confidentiality aspects. we trace the evolutionary process wherein the various security ideas were periodically refined in the light of emerging threats and attacks at every point of time. We also outline the role played by cryptology in achieving several of our goals but we will not dwell in the mathematical details. on the contrary, we argue, even with simple understanding, the right things to be done with crypto tools and discuss on the real world scenario where these ideas, principles and protocols are deployed.

14:30pm — **Day 1 Close**

CYBER RESILIENCY

CONFERENCE AGENDA

DAY 2: 18th Oct 2016

9:00am to 9:30am	**Networking & Refreshments**
9:30am to 10:00am	**Cyber Hacking –** by David A. Cass, Chief Information Security Officer, IBM Cloud & SaaS Operational Services
10:00am to 10:30am	**Cyber Resiliency Planning –** by Dhiraj Sasidharan, Director Compliance & I.T. Risk Management, Jumeirah Group The presentation will cover what an organization needs to be aware of in order to ensure Cyber Resiliency in their operations. It will cover certain planning, stakeholder engagement and simulation exercise strategies from a merchant perspective.
10:30am to 11:00am	**Metasploit framework – A pragmatic approach** – by KK Mookhey, Principal Consultant, NII Consulting
11:00am to 11:30am	**Networking Break with Tea/Coffee**
11:30am to 12:00pm	**TBD**
12:00pm to 1:00pm	**TBD**
13:00 to 14:00	**Lunch Break**
14:00 to 14:30	**TBD**
14:30pm	**Vote of thanks**

Schedule is subject to change without any notice

REGISTRATION
ISAFE 2016 Conference
(16th, 17th & 18th Oct 2016)

Name: _____

Organization: _____ Title: _____

Mailing Address: _____

City: _____ Mobile: _____

Day Telephone: _____ Email: _____

Name to appear on the badge_____

Registering as Member ☐ or as Non-Member ☐ (Please tick one)

ISACA Membership ID (if ticked as Member):_____

PRE LAUNCH REGISTRATION (on or before 30th June 2016)		Member (AED)	Non-Member (AED)	Tick One
Pre-Conference workshop only	1 Day (16 Oct 16)	1500/-	1800/-	O
Conference only	2 Days (17 & 18 Oct 16)	1500/-	1800/-	O
Conference & workshop	3 Days (16, 17 & 18 Oct 16)	2500/-	3000/-	O
EARLY BIRD REGISTRATION (on or before 1st Sep 2016)				
Pre-Conference workshop only	1 Day (16 Oct 16)	1750/-	2050/-	O
Conference only	2 Days (17 & 18 Oct 16)	1750/-	2050/-	O
Conference & workshop	3 Days (16, 17 & 18 Oct 16)	3000/-	3500/-	O
REGISTRATION after 1st Sep 2016)				
Pre-Conference workshop only	1 Day (16 Oct 16)	2000/-	2500/-	O
Conference only	2 Days (17 & 18 Oct 16)	2000/-	2500/-	O
Conference & workshop	3 Days (16, 17 & 18 Oct 16)	3500/-	4000/-	O

EASY STEPS TO RESERVE YOUR SEAT

STEP 1: Take a print out and fill in the above registration form

STEP 2: Prepare the cheque in favour of **Pivotal Consultancy** and request for courier pickup.

STEP 3: Please scan the registration form along with the proof of payment (eg: cheque) and email it to Ms Harneet on **harneet@pivotal.ae** or **isafe16@isacauae.org**. Please indicate the correct address, mobile number and a block of time (fourhours) to enable the courier company to pick up the cheque from you. For any other payment methods (online transfer or ATM deposit contact Ms Harneet)

For any other queries regarding the ISAFE 2016 and any other payment mode please contact **Ms Harneet: 050-8679196 between (10am - 6:00pm). SEATS WOULD BE RESERVED ON FIRST COME FIRST SERVE BASISAND ONLY AFTER YOUR PAYMENT IS RECEIVED. FEE ONCE PAID WILL NOT BE REFUNDED IN ANY CIRCUMSTANCES**. I have understood and agree with the conference details, terms and conditions. I would like to register for the same.

DELEGATEE SIGNATURE: _____ DATED: _____