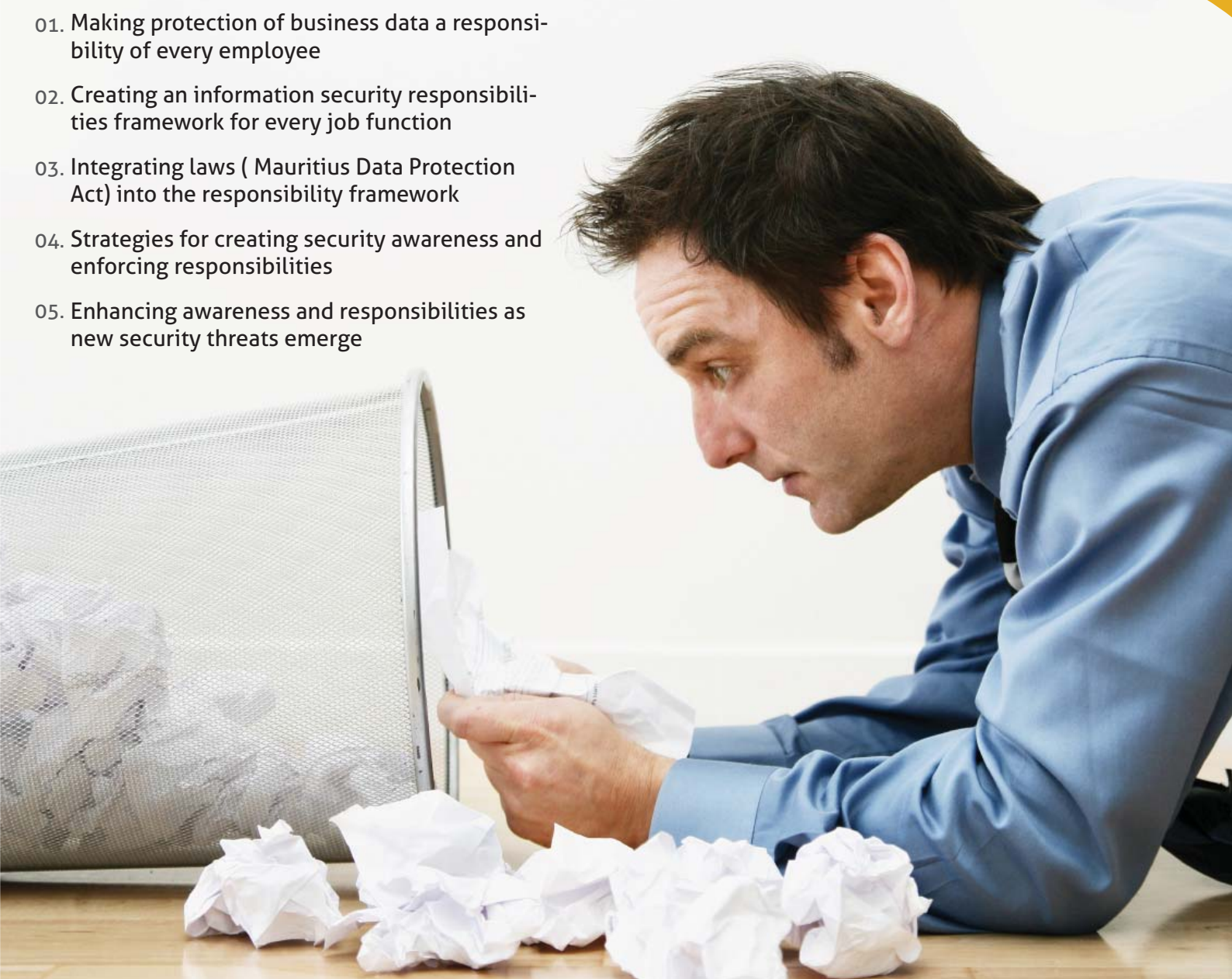


“Oops! I found my secret business data in the thrash can”

An Information Security Awareness & Responsibilities Implementation
Leader Training Certification Seminar

What will you learn?

01. Making protection of business data a responsibility of every employee
02. Creating an information security responsibilities framework for every job function
03. Integrating laws (Mauritius Data Protection Act) into the responsibility framework
04. Strategies for creating security awareness and enforcing responsibilities
05. Enhancing awareness and responsibilities as new security threats emerge



February 3, 4 and 5, 2010, Four Points By Sheraton Ebene, Mauritius



MULTIEVENTS
Your preferred Events partner
www.multievents.mu

Presented by

InterSecApp

International

Security

Applications

www.intersecapp.com

Program outline and syllabus

DAY 1 - February 3, 2010

Registration: Time – 08:00 to 08:30

Session 1: Interactive video and quiz: 10 top security mistakes an employee makes: Time – 08:30 to 10:15

Introduction: The human angle in information security

Delegate introductions: The “Being Honest Ice-Breaking session”:

Each delegate will make a short talk of 4 minutes on the theme – “The last time I shared my password ...” The delegate shall explain why they did it? What is the risk? And, can this be avoided?

Tea/Coffee Break: Time 10:15 to 10:30

Session 2: Case-study: The difference between information security “awareness” and “behavior”: Time 10:30 to 12:00

The delegates will learn from a real-life information security awareness project that created awareness amongst the employees but did not get the expected behavior.

Group activity: Each team shall explain,

- The reasons for the failure
- How they would have done things differently

Session 3: Creating an Awareness and Responsibilities Application Model for Information Security: Time 12:00 to 13:00

The delegates will create an Awareness and Responsibilities Application Model for Information Security

The structure and explanation of the model– Governance, Deployment, Verification, Improvement

Lunch: Time 13:00 to 14:00

Session 4: Introduction to the Governance Phase: Time 14:00 to 14:30

Structure of the governance team

Linking business requirements with user information security responsibilities, including contractual obligations, legal requirements, business practices etc.

Session 5: Information Security Responsibility Framework: Time 14:30 to 15:30

Introduction to the Information Security Responsibility Framework

Group activity: Each team will create the Information Security Responsibilities Framework which covers,

- General responsibilities
- Job specific responsibilities
- Vendor and contractor responsibilities

Tea/Coffee Break: Time 15:30 to 15:45

Session 6: Gap analysis: Time 15:45 to 17:30

Introduction to current state analysis techniques

Case study: The following techniques for current state analysis shall be discussed along with real-world case studies.

- Social engineering
- Observations
- Interviews
- Incident reviews

Group activity: Delegates shall define a measurement criterion for the findings from the current state analysis

- For information security awareness
- For information security behavior (application)

Day 2 - February 4, 2010

Session 7: Culture of the organization, strategies for awareness creation and responsibility enforcement: Time 08:30 to 09:30

Work culture of the organization and it’s impact on information security practices

Debate session: What works best, the soft approach or the hard approach for information security responsibilities enforcement? Delegate shall form two teams and present arguments on the debate theme.

Session 8: Creating Information Security Awareness and Responsibilities Policies and Strategies: Time 09:30 to 10:30

Case study: Creating information security responsibility policies

Group activity: Delegates shall create strategies for,

- Awareness creation
- Responsibility enforcement and/ or motivation

Creation of governance processes: defining inputs, defining actions on inputs, defining expected outputs and metrics

Tea/Coffee Break: Time 10:30 to 10:45

Session 8: Introduction to the Deployment Phase: Time 10:45 to 12:00

Creation of essential “deployment” processes

Coverage of deployment: Defining the coverage for information security awareness and responsibility enforcement, define the workforce constituents and their locations

Visibility of deployment: Define the visibility strategy, the channels for spreading awareness

Group activity: Measure the current level of,

- Information security awareness and responsibilities coverage
- Information security awareness and responsibilities visibility

Session 9: Quality and types of information security awareness content: Time 12:00 to 13:00

Case study: Awareness content creation: The 5 qualities of awareness content viz.,

1. Clarity
2. Cultural consideration
3. Impact visualization
4. User participation (Interactivity)
5. Retention measurement: Methods and strategy

Case study: Types of awareness content: advantages and disadvantages.

- Classroom training slides
- Animated videos
- Posters
- Mind-maps

Lunch: Time 13:00 to 14:00

Session 10: Build your information security awareness & responsibilities communication strategy and content: Time 14:00 to 15:30

Group activity: Each team shall perform the following activities.

- Awareness topic selection – Each team shall select 4 components from the Information Security Responsibility Framework
- Content definition – Each team shall make an outline of the content to be created for each awareness topic. The content must communicate the responsibilities and impact with clarity
- Content creation – Each team shall create 4 types of content for 4 awareness topics i.e. training slides,, animated video, poster and mind-map

Tea/Coffee Break: Time 15:30 to 15:45

Session 10: Build your information security awareness & responsibilities communication strategy and content (Continues) : Time 15:45 to 17:30

Day 3 - February 5, 2010

Session 11: Presenting and teaching information security awareness and communicating responsibilities: Time 08:30 to 10:15

Group presentation – Each team shall present the information security awareness content that they have prepared to the rest of the delegates. The content shall be rated based on the 5 qualities of awareness content

Definition of essential processes of the deployment phase

Tea/Coffee Break: Time 10:15 to 10:30

Session 12: Introduction to the Verification Phase: Time 10:30 to 12:00

Definition of essential verification processes

Verification strategies (linked to current state analysis from Governance Model)

Group activity: Define 4 verification (audit) strategies that are linked to the Information Security Responsibilities Framework,

- Social engineering
- Observation
- Interviews
- Incident / Log reviews

Quantification and scoring of audit (verification) findings

Group activity:

Each group shall explain how their verification strategies differ from the initial verification strategies used in the “Governance” phase

Session 13: Introduction to the Improvement Phase: Time 12:00 to 13:00

Definition of essential improvement processes using the inputs from,

- Audit findings
- New security incidents and events from the industry
- New business practices, requirements
- New legal requirements

Lunch: Time 13:00 to 14:00

Session 14: Role play session: Senior management review of audit findings: Time 14:00 to 15:30

Group activity: A review team shall be formed amongst the delegates and the review team shall evaluate the audit findings. Based on the findings, the review team shall recommend actions for,

- Improving the Information Security Responsibility Framework
- Improving strategies for awareness creation
- Improving strategies for responsibility enforcement

Tea/Coffee Break: Time 15:30 to 15:45

Session 15: Certification Exam: Time 15:45 to 17:00

A 60 minute, 30 questions, multiple choice test shall be administered at the end of the course for all candidates. The test shall be paper-based with a set of multiple choice questions focusing on the topics covered during the course. The test results shall be conveyed to all candidates within 7 days of course completion. All candidates who successfully pass the test shall be awarded the “**Certified Security Awareness and Responsibilities Implementation Leader**” certificate by International

Conclusion: Time 17:00 to 17:15

Award of Certificate of Attendance: Time 17:15 to 17:30

End of seminar: Time 17:30

Profile: Anup Narayanan

Anup Narayanan is an information security professional with more than 10 years of experience. He is a CISA & CISSP and the principal author of HIM-IS (Human Impact Management for Information Security). Anup is the Managing Director of First Legion Consulting, which specializes in information security awareness and behavior management solutions and the founder of International Security Applications, which focuses on information security compliance. He is the creator of ISQ World, an information security awareness management services portal. His clients for information security awareness and behavior management solutions include Ericsson, Vodafone, UST Global, OnMobile Global, J Kalachand & Company, and Lakshmi Machine Works. His training and speaking experiences covers India, Mauritius, Spain, Portugal and Vietnam. Anup is a contributing author of “Social and Human elements of information security” and the principal author for “Information Security Management” course book for NIIT. Prior to becoming an information security entrepreneur, Anup worked in information security positions for HCL Comnet and Global e-Secure.

Anup can be contacted at: anup@intersecapp.com.

Testimonials about Anup’s training can be found at www.intersecapp.com.

About Multievents

Started in 2008, Multievents has since grown and continues to do so by 'Making the impossible possible'. That's our motto we take while producing events every year. Since 2008, we've been producing and managing corporate events, conferences, workshops & seminars and conventions for a wide array of clients. And our goal remains the same—to bring people together—to share, learn, network, to inform, to inspire, to promote business and to build relationships, face-to-face.

We offer timely business critical information, insights and analysis conducted by industry practitioners and academics to provide participants a well-balanced blend of theoretical fundamentals and practical applications over a wide array of professional topics. For more information contact us on contact@multievents.mu

5 EASY WAYS TO REGISTER:

- 1 Phone: +230 290 5050/ +230 670 9744
- 2 Fax: +230 290 5060 (By completing the registration form)
- 3 Email: registration@multievents.mu
- 4 Website: www.multievents.mu
- 5 Post: Mail your completed registration form along with payment to: Multievents Ltd, Angle Rues Ritter et T. D'Arifat, Curepipe

Multievents your preferred events partner!

To see our range of events, and to find out how we can organise an event for you, visit

www.multievents.mu

or by email contact@multievents.mu

Terms and Conditions of participation

Registration

Reservations may be made by telephone/telefax/email/online but will only be confirmed upon receipt of the relevant registration form(s) and payment of the registration fee of Rs. 19,500/- per delegate.

Payment By Cheque: All cheques should be crossed, marked A/C payee only and made payable to "MULTIEVENTS LTD" and mail to Multievents Ltd, Angle Rues Ritter & D'Arifat, Curepipe.

Payment must be received by us at **latest one week before** the date of the workshop.

Cancellation and Substitution Policy

A substitute delegate is welcome at any time at no extra charge if the registered participant is unable to attend. Cancellations received until Jan 20th, 2010 will be assessed a Rs 1500/- administrative fee. 50% of the registration fee will be refunded for cancellations received from Jan 20th to Jan 25th 2010. 100% of the registration fee is applicable for cancellation received after 25th January 2010. This also applies to no show on the day of event. All notices of cancellation or replacements must be made in writing and acknowledged by Multievents Ltd. via email or fax.

Programme Changes

Multievents Ltd reserves the right to amend or cancel the event due to unforeseen circumstances or 'force majeure'

Registration Information

Contact person: Sonia/Isabelle

Address: Angle Rues Ritter et T. D'Arifat Curepipe

Tel: 670 9744 / 290 5050 Fax: 290 6050

Email: registration@multievents.mu

Website: www.multievents.mu

Organised By

Sponsor

Media Partner

Online Media
Partner



MULTIEVENTS
Your preferred Events partner

