Val-Ed™

Valiant Technologies Education & Training Services

Security Awareness for IT Users

Welcome to Valiant Technologies. We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. With significant strength also in information security assurance services, Valiant CISSTech, as we were formerly known, has been serving clients across many countries - Bahrain, Hong Kong, India, Kuwait, Malaysia, Maldives, Saudi Arabia, Sri Lanka, South Africa, Sultanate of Oman, Thailand, United Arab Emirates, and Zambia.

Val-Ed™, our educational services division offers a variety of ready-packaged and tailor-made educational and training programs in the area of information security. This catalogue provides detailed information on one of the educational and training offering to clients in the area of information security technology, management and assurance.

We have a full range of services that we offer covering the full spectrum of information security and our services catalogue provides details of the following services that we provide to clients. Please ask for a services catalogue for more details on these services:

- Testing and hardening of information system defenses:
  - Vulnerability assessment
  - Penetration testing
  - Application security testing
  - Hardening of servers and network components
  - Periodic evaluation of network security
- Information Security Management Services
  - Security Policies, Procedures and Guidelines
  - Security Awareness Program
  - Risk Assessment and Analysis
  - Executive Management briefings on Security
  - Vendor selection for security products
  - Computer Forensics Investigation\
  - ISO-27001 preparatory services
  - Fill-in Security Manager program
- Control and Assurance Services
  - Gap analysis against ISO-27001, COBIT, ISSAF
  - Information security controls review
  - Information Systems Security Audit
  - Control assessment for SOX compliance
- Business Continuity and Disaster Recovery Management

We look forward to being of service to you and look forward to hearing your interest.

- Valiant Team

List of regular programs offered by Valiant Technologies

	Course Name	Duration (days)
1	Workshop for CISSP Aspirants	4
2	Workshop for CISA Aspirants	5
3	Workshop for CISM Aspirant	4
4	Workshop on BCP and DRP	2
5	Workshop on Change Management	1
6	Workshop on Information Security Policies	3
7	Information Security for Senior Management	½
8	Security Awareness for IT user management	2
9	Security Plus Certification of CompTIA	6
10	Sarbanes Oxley Act – Structure and Implementation	2
11	Digital Evidence for IT / IS Auditors	1

CV of principal instructor, Dr Rama K Subramaniam is found on the last page

Awareness workshop on Information Security
for IT user management

Why?

User management is not only expected to protect information assets but are also expected to put in place a clear program to implement enterprise-wide information security policies aimed at minimizing the harmful effects when information assets are affected.

User managers need to address issues of information security infractions as seriously as they would address loss of physical assets of strategic importance. Various independent surveys have pointed to the increasing budget allocation for securing information assets. With the concept of due care becoming more prevalent in information based decision systems, executive management is often tested on the five elements that constitute due care, *viz.*,

- gravity of harm,
- likelihood of occurrence,
- cost of preventing the harm,
- duty of care and
- standard of care.

Implementing and demonstrating due care requires that executive management sets a clear techno-commercial framework for handling security of information assets. This program helps managers create, adapt and use such a framework.

What?

This program will create technological awareness of information security among user managers and present them with the state-of-the-technology solution overviews they can choose from and implement in their organizations.

The program would not require participants to have in-depth technology knowledge and would aim at:

- bringing the participants up-to-date on the managerial issues involved in evaluating from amongst alternative approaches to securing information assets
- the risks and benefits of various approaches,
- the degree of security they could establish while approving implementation of specific solutions and
- the need for an enterprise-wide approach to information security.

Day – 1

Day theme: The first day of the session would consider strategy level information security issues and set the tone for study of solutions and implementations to be considered on the second day.

Session – 1: Security Policies – design and implementation

Background: Good information security program starts with sound security policies. Creating and implementing a comprehensive and structured security policy across the enterprise assists all stakeholders in the business to meet their objectives. It demonstrates management commitment to information security and provides direction when operating management has to decide on issues relating to safeguarding of information assets either in the normal course of business operations or in a crisis.

Deliverable: This session would assist the participants to create enterprise-wide information security polices and takes them through the steps required to implement it successfully.

Session – 2: Information risk management

Background: A number of methodologies have been validated for carrying out information risk management. Often managers make investments in time, money and technology without effective risk management thereby increasing their exposures through installation of technologies that are not scalable, not compatible and offer short lifecycles. The result is an insecure information infrastructure despite all the costs and efforts

Deliverable: This session would present some of the good methods of risk management available and consider the NIST methodology in detail

Session – 3: Business Continuity and Disaster Recovery Planning

Background: Businesses are rapidly increasing their reliance on information processing systems and information technology driven decision processes for creating and sustaining strategic competitive advantage. In addition, many regulatory and legal compliance requirements require the use of large processing capacity often found only on high-end information processing facilities. Information security that includes "availability" requires managers to be put in place a structured methodology to respond to disasters and events challenging business continuity.

Deliverable: This session would present a structured approach to creation, testing and maintenance of business continuity and disaster recovery plans

Session – 4: Securing the Systems Development Life Cycle

Background: Security being a new entrant to the system requirement specification (SRS) process, it is often considered as an add-on to application systems that are developed to fully meet functionality and quality standards. These result in security patches to be added to applications that often do not fully integrate with functionality and more dangerously do not seamlessly integrate with the processing flow.

Deliverable: This session would present the various security requirements that needs to be integrated into the different stages of systems development life cycle (SDLC) by considering each stage of the life cycle irrespective of the SDLC methodology adopted.

End of day – 1 sessions

Day – 2

Day theme: The second day of the program would discuss operations level information security issues from a managerial perspective. These sessions would consider products generically and would be vendor-neutral in nature.

Session – 5: Securing data in storage and in transit over networks

Background: Data while stored or while in transit over networks is subject to a variety of attacks that destroy their confidentiality and integrity apart from raising questions about the authentication of source of the message conveying the information that could be used for key decision process. In addition, managers would need assurance on the authenticity of the message itself apart from meeting the legal requirements of non-repudiation in an e-commerce environment.

Deliverable: This session would look at the emerging technologies offering assurance of confidentiality and integrity of data in storage and in transit and address issues of PKI and digital signature

Session – 6: Perimeter Security

Background: The information processing facility (IPF) and the networks all operate within a logical perimeter that is violated whenever a security infraction originates from outside the IPF. The need to secure the perimeter has been addressed by many methodologies and with different goals. Managers need to necessarily secure their information and processing assets at the perimeter as a first line of defense.

Deliverable: This session would introduce the participants to the fundamentals of Firewalls, IDS and anti-virus management systems. Participants would also be acquainted with the basics of networking to the extent they need familiarity to understand the technologies being discussed

Session – 7: Awareness and Training

Background: Global surveys by different organizations have repeatedly brought out the fact that around two-thirds of security infractions originate from sources internal to the system. While malicious intent contributes towards this, the curious but ignorant contribute much more. It may be difficult to rein-in the former but the latter can be eliminated via awareness and training

Deliverable: This session would address awareness and training issues relating to information security and present a blueprint for creating and implementing an enterprise-wide awareness and training program

Session – 8: Standards, metrics and road map for creating a secure enterprise

Background: Security is too wide to be straight jacketed into a single corporate or implementation model. The need for multiple approaches to information security lends credence to the need for creating and implementing global standards, baselines and best-practice statements. ISO-17799 is emerging as the ubiquitous standard for implementing security management systems while COBIT is being endorsed as the most appropriate collection of best practices. Apart from these, standards are emerging from a number of organizations at the component, device and service levels. Managers would do well to be aware of these standards intended to assure them of a minimum level of performance guarantee.

Deliverable: This session aims at familiarizing participants with popular and relevant global standards and best practice guidelines relevant to information security products and services

End of Program

Principal Instructor

Dr. Rama K Subramaniam

MBA(UK), PHD, FCA, CISA, CISM, CISSP, CEH, CHFI, CSQP, MCSE, Security+

He is Director of Valiant Technologies Pvt Ltd and Tejas Brainware Systems Pvt Ltd. He has been an information security consultant, trainer and educator for over a decade now. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He has also been a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He is a certified and experienced professional in the areas of creating and implementing secure information security architecture; internal controls systems and processes; conceptualization, creation, testing and maintenance of business continuity and disaster recovery plans; security audits and certification of network infrastructure; conceptualization and implementation of multi-factor authentication processes (including PKI and X.509 compliant certification infrastructure); creation, assessment and certification of CoBIT, ISO-17799, BS-7799 and ISO-15408 compliant information security management systems.

He served earlier as Global Chair of the Education and Awareness Principles Expert Group of Globally Accepted Information Security Principles (GAISP), based in the United States and is currently Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he overseas their certification and accreditation processes. He is the charter President of the first chapter of ISSA (Information Systems Security Association) in Asia and served on the boards of Dubai and Chennai chapters of ISACA. He is past Co-Chairman of the Information and Communication Technologies Expert Committee of the Hindustan Chamber of Commerce and charter President of Institute of Internal Auditors, Zambia.

He was formerly Managing Director of Thewo Corporate Services based in Lusaka, Zambia; Group Operations Director or Benetone Group of Companies based in Bangkok, Thailand and Commercial Director of Dynaspede Integrated Systems Ltd, based in Mumbai.