Thought Leadership...

Valiant Technologies

Val-Ed™

Valiant Technologies Education & Training Services

Executive Management briefings on Information Security

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 certification aspirants	4
2	Workshop for CISA certification aspirants	5
3	Workshop for CISM certification aspirant	4
4	Workshop for CBCP certification aspirants	5
5	Workshop for Security+ certification aspirants	6
6	Workshop on BCP and DRP	2
7	Workshop on Change Management	1
8	Workshop on Information Security Policies	3
9	Information Security for Senior Management	½
10	Security Awareness for IT user management	2
11	Ethical Hacking and securing your networks	6
12	Sarbanes Oxley Act – Structure and Implementation	2
13	Digital Evidence for IT / IS Auditors	1
14	IS Audit: Principles and Practices	3
15	ISO 27001: Process and Implementation	5
16	Auditing Information Technology	3
17	Management for Technology Professionals	3

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

Workshop on Information Security
for Senior Management

Why?

Management is not only expected to protect information assets but are also expected to put in place a clear program to minimize harmful effects when information assets are affected. In addition to the cost of technological repair to information assets, managements need to be cautious of degradation of reputation, loss of strategic competitive advantage and where appropriate, erosion of market capitalization.

Managements 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.

Implementing and demonstrating implementation of 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 business 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.

Scheduling:

A half day (approximately four hours) program is being presented with five sessions each of 45 minutes duration. Each of the sessions would be made as interactive as possible encouraging participants to discuss their real-life scenarios.

Session – 1

Information security as a driver for strategic competitive advantage

Background: Over a period of time drivers for strategic competitive advantage have changed in keeping with the changing business scenario. Arguably, information is the most important driver of strategic competitive advantage now. This session presents information in a non-technical perspective and focuses on the business importance of information, as a key asset. Given that information is a strategic corporate asset, the need to secure it like any other strategic corporate asset needs no over-emphasis.

Coverage:

- Information – tangible and intangible values
- Current technological horizon for securing information
- Multiple paradigms in understanding information security
- Rationalization, globalization and standardization
-

Session – 2

Information Security Policies

Background: The primary responsibility of top management vis-à-vis information security is to create a secure information processing facility (IPF). Creating a secure IPF involves action at strategic, operational and implementation planes. Top management must push information security from the board level down right through to operations. The sure way of doing this with the required degree of consistency and emphasis is the creation and implementation of enterprise-wide security policies. Good security polices assist operational personnel to respond effectively to information security infractions in a speedy and pre-determined manner. Security policies also serve as the medium through which top management clearly demonstrates its commitment to information security.

Coverage:

- Creation
- Implementation
- Checklist for successful implementation of security policies
- Importance and usefulness

Session – 3

Risk Management Systems

Background: Risk management, as applied to information technology systems, encompasses the process that allows IT managers to balance operational and economic considerations of various forms of controls with increased security of key information system capabilities. It is normally done through protecting information processing facilities and the date that is stored within and that which is in transit across the systems.

As with every other risk management paradigm, information technology risk management is a three-phase process – risk assessment, risk mitigation and risk evaluation & assessment.

Coverage:

- Risk Assessment
- Risk Mitigation
- Countermeasures and controls

Session – 4

Business Continuity and Disaster Recovery Planning

Background: Business Continuity Planning and Disaster Recovery Planning (DRP) are used to describe activities designed to manage risk by reducing the likelihood and the impact of a physical disaster or any significant service interruption. In addition, plans are developed to enable resumption of critical business functions and support operations when a disruption occurs. Business Continuity Planning applies to recovery of business functions; Disaster Recovery Planning applies to recovery of IT services, voice and data communications systems in support of the business functions. Top managements are mandated by virtue of their need to secure information processing facilities to plan for any eventuality and have a clear course of action to recover operational capabilities as soon as feasible. This is achieved through a well orchestrated plan adequately tested and maintained

Coverage:

- BCP vs. DRP
- Business Impact Analysis
- Recovery Strategy selection and implementation
- Testing BCP and DRP
- Maintenance of BCP and DRP
- Operational and Strategic issues

Session – 5

Enterprise-wide information awareness program

Background: It is now well established beyond any doubt that technology driven solutions will not provide a counter-measure for all known attacks against information assets and infrastructure. Often it is the well-trained, sufficiently motivated and informed employee who is the best defense against exploitations of vulnerabilities. Top managements would do well to create and implement a structured enterprise-wide awareness program that would reach every level of the organization, which uses or interfaces information. Such a program requires support – both budgetary and motivational – from top management. This session would present framework for creation and implementation of such a program

Coverage:

- Creation of programs
- Content of programs
- Implementation
- Follow up and evaluation of effectiveness

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. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He is a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He serves as India's country representative at International Federation of Information Processing (IFIP), serving on their Technical Committee TC-11 dealing with information security. He is current Chairman of ISCCRF, a not-for-profit trust carrying out research in cyber crime management

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 SOX, COSO, CoBIT, ISO-27001, ISO-17799 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 former Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he estblished 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 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.