Thought Leadership...

Valiant
Technologies

Val-Ed™

Valiant Technologies
Education &
Training Services

Workshop on
Information Security
Policies

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 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

Three day workshop on Information Security Policies – creation, implementation and follow-up

Why?

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

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*:

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

Demonstrating due care requires that executive management sets a clear techno-commercial framework for handling security of information assets. This program helps participants to create, adapt and use the foundations of such a framework.

What?

This workshop takes the participants from the stage of creating a framework for information security policies right through to implementation, and includes some key steps like "selling" the idea to top management, generating consensus on security objective, establishing cost-benefit relationships for policy implementation and development of policy contents. Participants in this workshop would actively participate in the development of sample policies that are relevant to their enterprises.

The program would address some key questions relating to Information security policies:

- What is an enterprise-wide information security policy?
- Why should such a policy be formalized in any enterprise?
- What should an information security policy contain?
- Why should any enterprise implement an effective information security policy?
- Can an enterprise get on with "informal" or "friendly-format" information security policies and still achieve the required degree of security?
- Are regulatory reasons driving policy creation and implementation?

How?

The program, on all three days would consist of structured presentations in the forenoon sessions. All afternoon sessions would be hands-on sessions where the participants would develop security policies specific to their organizations and build up the set of policies for them to take back and implement in their enterprises.

Day – 1

Day's theme: The first day of the session would consider strategy level information security issues and set the tone for study of policy considerations and implementation issues to be considered later in the program.

Forenoon Sessions

Session – 1: Security Policies – overall design

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 the overall inventory of content for an enterprise-wide information security policy and take them through the steps required to implement it successfully.

Session – 2: Information security Policies – types and approaches & generic issues

Background: A number of methodologies have been validated for creating information security policies. Often managers make investments in time, money and technology without an effective and relevant framework to synergize the strengths of administrative, technological and physical controls acting together against identified vulnerabilities. The result is an insecure information infrastructure despite all the costs and efforts expended.

Deliverable: This session would present some of the good methods for structuring policies at different levels like General Program Policies, Topic Specific Policies and System and Application specific policies. In this session, participants would identify the full list of areas that require information security policies. This list would be divided into generic and technology specific policies. This session would also discuss issues of maintaining and updating policies along with testing process to keep them relevant and up-to-date.

Afternoon Sessions

Participants would work on the creation of table of contents for a security policy that has generic content and each participant would add areas that are relevant to their specific organization. In this exercise, a template of generic policy headings would be provided to the participants for adapting to their specific environments.

Participants would write out the generic information security policies that would be applicable to most enterprises and discuss the issues relating to implementing generic policies at the enterprise level.

Deliverable

At the end of the first day, all participants would have a full table of content for their security policy and would have written generic policies that are applicable across organizations and are generally same for organizations with near equal risk profile at an organizational level.

End of day – 1 sessions

Day – 2

Day's theme: The second day of the session would consider operating level information security issues that are driven by the technology implementation and the organizational security architecture. Participants would focus on creating security policies for technology specific environments.

Forenoon Sessions

Session – 3: Perimeter Security

Background: The information processing facility (IPF) and all components of networks operate within a logical perimeter constituting the Trusted Computing Base (TCB). This 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 content and IPF assets at the perimeter providing a first line of defense.

Deliverable: This session would introduce the participants to policy issues in respect of Firewalls, IDS and anti-virus management systems. Participants would also be presented with basic policies related to networking architecture.

Session – 4: 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. 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 authentication and assurance of confidentiality and integrity of data in storage and in transit and address issues of contemporary interest like PKI and digital signature. The session would consider policy initiatives on common areas like multi-factor authentication (both technological and administrative issues), convergence of identity management approaches, proprietary approaches and integrating them into open source implementations, etc.

Afternoon Sessions

Participants would identify the policies relating to perimeter security and those pertaining to security of data in storage and while in transit over networks. In respect of these two areas participants would use templates to create policies relevant to their organization. Participants would also go through instructor moderated discussion on the relative relevance, cost-effectiveness and applicability of different objectives in the areas considered during forenoon session

Deliverable

At the end of the second day, all participants would have a full set of security policies covering technology and applications that are primarily installed for providing a first level of defense at the TCB perimeter. The second day end would also see participants designing policies for protecting their data in storage within their IPF and when such data moves within the IPF or across networks interfacing with their IPF.

End of day – 2 sessions

Day – 3

Day's theme: The third day of the session would consider management controls in the areas of secure systems development process and planning for business discontinuity events and disasters.

Forenoon Sessions

Session – 5: 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. One of the key drivers for information security to enter the SDLC is a strong push at the policy level.

Deliverable: This session would present the various security requirements that need 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. For security issues to be considered at each SDLC stages, policy issues that are relevant will be discussed.

Session – 6: 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 warrant the use of large processing capacity often found only on high-end information processing facilities. Information security considers the "availability" attribute as significant and 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 policies related to creation, testing and maintenance of business continuity and disaster recovery plans. The session would also consider policy initiatives appropriate to sustain appropriate availability of systems and data.

Afternoon Sessions

Participants would identify the policies relating to the key components of systems development / acquisition processes. This being an area which, if handled without adequate reference to security, can lead to long term damage to information systems needs significant policy directive and strong management controls in place. Participants would go through a structured process of assessing security requirements in each of the major stages of systems development / acquisition process and develop policies for securing each of these stages.

In addition, participants would evolve policies directing the planning for business discontinuity events / disasters. While organizational requirements for such planning may vary, participants would cover basic common grounds derived from “best practices” in the BCP and DRP security policies.

Deliverable

At the end of the third day, all participants would have a full set of security policies covering all stages of system development / acquisition processes [including initiation, process, testing and maintenance] along with policies for an on-going certification and accreditation of systems and applications from a security perspective. Participants would also decide on polices that would initiate, exercise, test and maintain business continuity and disaster recovery plans.

End of day – 3 sessions

Overall program deliverable

The three day highly interactive and participation-intensive workshop would provide every participant with a good conceptual foundation and where appropriate, hands-on experience in respect of the following issues relevant when designing, implementing and maintaining information security policies:

- The need for a policy
- Evolving a policy framework
- Policies, Standards, Procedures and Guidelines
- Mapping the security framework of the organization
- Cost-benefit analysis of security activities
- Getting top management to "buy" security policies
- Creating a detailed policy
- Implementation, compliance and monitoring
- Security awareness program
- Testing, maintaining and updating the policy
- Hands-on exercise for skill development in security policy creation

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.