CASE STUDY SET 2

**VIKRAMADITYA REDDY VARKALA**

**Z1973679**

**CASE STUDY 4: IBM:THE EMBEDDED SECURITY SUBSYSTEM**

**Q1)Why is it essential to have a hardware security foundation?**

Hardware security is an important aspect of modern computing system. Hardware security can help protect against various types of threats, it helps :

* From insider threats
* To protect against Remote attacks
* To prevent Data breaches
* To Ensure compliance with Industry standards
* To provide secure user authentication

**Q2)Identify at least five attacks that cannot be defended with software.**

Five attacks that cannot be defended with software are:

* Physically accessing a system to steal sensitive data.

Ex: stealing a laptop or server to access a system's ports to install malware or extract data.

* Hardware-based attacks:

Ex: inserting malicious code into a system

* Tricking users into divulging sensitive information

Ex: using phishing emails or phone calls to trick users into revealing their passwords or other sensitive data.

* Inserting malware into a software update or firmware before it is distributed to customers.
* Physical disasters like fire, floods etc.
* Intentionally injecting faults into a system to cause it to behave in unexpected ways.

**Q3)Why are open standards important in security?**

Open standards are essential for ensuring strong security measures in today's interconnected world. Open standard are important in security

* When creating security metrics, it is important that test methodologies cover multiple scenarios to ensure that devices perform as expected in realistic environments.
* An open testing standard allows everyone to see what is tested and how it’s tested so that the users can be confident that they are secure and free from hidden vulnerabilities.
* Open standards allows developers to build upon existing standards and create new versions to improve security.
* Open standards allow different security technologies and products to work together consistently hence ensure security from threats.

**Q5)What does trusted computing mean?**

Trusted hardware is the foundation for trusted systems. Trusted computing aims to increase the security by establishing a trustworthy environment between hardware and software components that work together.

IBM's ESS 2.0 chip provides stronger user authentication, device validation, and system integrity, and therefore greater system trust.

Trusted computing enables features such as secure boot, secure storage, and secure communications which help to protect against malware, phishing attacks, and unauthorized access.

Trusted computing can be applied in :

* Cloud computing
* Mobile devices
* IOT devices
* High-security applications
* Military and government systems.

**CASE STUDY 5: SRA INTERNATIONAL, INC.**

**Q1)Why do you think SRA has chosen to focus its efforts on federal government departments and agencies within the national security market? Explain why this has been a good strategy for SRA.**

For federal agencies it is mandatory to verify compliance with government information security regulations but it is a time-consuming and complicated task.SRA knows well that there is very much scope for its growth if it works with federal government departments and its agencies .SRA International’s Web-based risk assessment software can automate the compliance process for federal government agencies .Thus, SRA has chosen to focus its efforts on federal government departments and agencies within the national security market.

This strategy has proven itself to be a good strategy for SRA because most of the revenue generated by the company is from the national security market.The company's 2005 reported net income was $57,723,000 on total revenue of $881, 770,000. Federal government clients accounted for ninety nine percent of the company's revenue: 60% was derived from national security clients, 29% from civilian agencies and departments, and 10% from health care and public health clients.As of June 30, 2005, SRA's backlog (orders for services under existing signed contracts) was approximately $2.7 billion.

**Q2) What is open source intelligence? What is tie relationship between open source intelligence, national security, and text and data mining software? Why should businesses be concerned about open source intelligence?**

Open source intelligence involves collection, analysis, and dissemination of intelligence gathered from publicly available sources like newspaper, magazines, journals, social websites, etc.

Text and data mining operations can extract and analyze massive amounts of data including those from open sources to identify patterns of activity, trends and correlations quickly and efficiently.

As Open source intelligence is gathered or achieved by text and data mining software hence the nation’s security is improved by these tasks.This can provide valuable information for threat assessments, monitoring of foreign governments and organizations, and identification of potential security risks.

Businesses should be concerned about open source intelligence as it can be to check the new and latest market trends, business can create business and marketing strategies as per the current trends and identify potential risks to the organization.

**Q3)What are critical infrastructures .List the U.S, critical infrastructure sectors and provide examples of each.**

Critical infrastructures can be assets, systems or resources either virtual or physical which are highly important to nation’s security. Any problem to these systems may affect badly on the economic security and safety of the nation.

SRA supports and develops the plans, programs, and operations needed to protect the nation's physical and cyber infrastructures from attack or disruption. SRA also assists the Defense Advanced Research Projects Agency's Tactical Technology Office in evaluating technologies developed by industry, universities, and military laboratories.

SRA supports the DoD information systems used by the Office of the Secretary of Defense, the defense agencies, the Joint Chiefs of Staff organizations, the three military departments (Army, Air Force, Navy), the four military services (Army, Air Force, Navy, Marine Corps), the National Guard, and the command structure. SRA's responsibilities typically involve the design, development, integration, and implementation of large, complex information systems.

SRA also provides IT support to the Army Reserve Component.

**Sectors:**

National Security Representatives:

* Department of Defense:Air mobility command,Army National Guard, Defence Manpower Data Center ,etc.
* Department of Homeland Security:
* Various Intelligence agencies

Civil Government Representatives:

* Department of commerce
* Us agency for international Development
* General services administration
* National Aeronautics and space administration etc.

Healthcare and Public Health Representatives:

* Army Medical Command
* Centers for Disease control and Prevention
* Food and Drug Administration.
* National Institutes of Health etc.

**Q4)﻿﻿﻿Why is improved interoperability between federal agency systems necessary for national security purposes?**

Associated with SRA's many services and solutions is the requirement that all federal agencies and their contractors must comply with government security regulations. Since 2002, compliance with the provisions set forth in the federal Information Security management act (FISMA) has been mandatory as its treated as a matter of national security. FISMA requires each Federal government agency to develop, document and implement and agency wide program to protect agency information and information systems.

The improved interoperability between the federal agency systems is necessary for national security purposes because

* Federal agencies need to work together to address emerging threats and challenges.
* Interoperability can help optimize resource allocation and utilization across agencies.
* Interoperability between federal agency systems can enable seamless sharing of information, data, and intelligence among agencies.

When all the systems are following same hardware and software standards, the integration of the systems and the communication between them becomes easier and more convenient, since data becomes easier to handle, it will also increase the security standards of the entire system.

**Q10)Explain how ASSERT's questions could be used by a business to better control its IT systems and to mitigate its security risks.**

ASSERT stands for Automated Security Self Evaluation and Remediation Tracking.It is based on the oracle database integrated with Macromedia’s ColdFusion.

ASSERT displays each assessment question in context and allows system owners to easily navigate between questions. Once the questions have been answered for the first time, future evaluations require considerably less effort. ASSERT uses the prior year's responses as a baseline to pre fill and inherit answers wherever possible, reducing the time required to complete the assessment process to approximately two hours a year.

ASSERT automatically generates remedial action plans based on the assessment answers. It links each remedial action plan to the information asset and to the business unit that owns it, and it identifies the assessment questions that generated each remedial action plan. It also provides the basic steps needed to remediate each identified vulnerability, along with the name of the individual responsible for each step.This makes it easier for managers at each agency to track the progress of their corrective actions.

From the assessment responses, ASSERT creates a centralized database of security data associated with an agency's information systems (eg. points of contact, date of latest approved security plan, information sensitivity classifications, resource needs). It also identifies risks to those systems, and provides current information on the status of the agency's security controls and remedial action plan initiatives. This information allows responsible managers to know the status of their systems at any point in time, enabling them to quickly institute necessary security improvements.

ASSERT incorporates the eight information security program requirements mandated by FISMA

* periodic risk assessments
* risk-based policies and procedures
* system security plans
* information security training
* periodic testing and evaluation of security policies
* remedial action plans
* security incident procedures
* continuity of operations plans.

Thus business can use ASSERT's questions to better control its IT systems and to mitigate its security risks.