CPP NOTES INFORMATION SECURITY

What is “rogueware”? Software that pretends to enhance security but compromises a computer

The cost of a theft of a trade secret by a cyberthief is best represented by which statement?

The value of the trade secret to the victim

Which are critical success factors that an information systems security standard must meet?

Executive oversight, periodic risk assessment, physical and personnel security

Which of the following terms is defined as “the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of the organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings”? CONVERGENCE

The convergence of physical and information security has numerous definitions. The Alliance for Enterprise Security Risk Management provides this basic definition (Booz Allen Hamilton, 2005): the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.

**Risk Management Approach to Information Assets Protection (IAP)**

All organizations possess and use information assets that warrant protection. The nature of that protection should be based on a sound risk management approach.

The following is a risk assessment process for use in IAP:

* Identify information assets.
* Valuate information assets (assigning a quantitative value, such as dollars, or a qualitative value, such as high, medium, or low).
* Assess threats to information assets. Assess likely adversaries.
* Assess the likelihood of occurrence of threats.
* Identify existing and projected vulnerabilities.
* Assess the impact of a loss event or disclosure on the organization.
* Identify existing and planned security controls or other options for addressing risk.

Which type of information security threats are most difficult to identify? INADVERTENT THREATS

Which of the following is the best example of good records-handling processes?

Routinely destroy all documents at set time periods

Which of the following is an example of a good process for information privacy?

Provide a mechanism to investigate compromises of privacy information.

\*\*\*GREAT PHRASE ASIS International holds that security is a business function.

Which security approach is defined as “viewing the big picture and identifying any protection gaps that remain despite current security measures”? OPSEC

Generally, which property rights have the longest duration? TRADE SECRETS

* **Sanitizing information systems and media**. Sanitizing is the process of removing data on a storage medium (such as a hard drive) before the medium is reused. Methods include overwriting and degaussing (magnetic erasure). An alternative is physical destruction.

Integration of custom code, third-party software, and servers that may create vulnerabilities involves what type of security? APPLICATION SECURITY

Realize that the two primary elements of recovery are **(1) to return to normal business operations as soon as possible and (2) to implement measures to prevent a recurrence** of the problem.

Management, policies, standards, personnel screening, and guidelines are examples of what type of countermeasures? ADMINISTRATIVE CONTROLS

Vulnerability and patch management, system monitoring and log review, and information systems security metrics are examples of what type of countermeasures? INFORMATION SYSTEMS INFRASTRUCTURE MANAGEMENT COUNTERMEASURES

One mechanism IT professionals use for managing their work is the IT Infrastructure Library or ITIL (pronounced “eye-til”). This is a framework developed by the British Office of Government Commerce in the 1980s. It has since been adopted as an international standard for managing IT. The standard addresses the concept of a service-level agreement (SLA). This is the way one negotiates with IT professionals for the services an organization needs to have delivered.

What is the IT Infrastructure Library? A STANDARD THAT ADDRESSES SEVICE-LEVEL AGREEMENTS

Who developed the CISSP Common Body of Knowledge? ISSA INFORMATION SYSTEMS SECURITY ASSOCIATION

**Gramm-Leach-Bliley Act**

–

In 1999 Congress passed the Gramm-Leach-Bliley Act, which regulates the use and disclosure of nonpublic personal information about individuals who obtain financial products or services from financial institutions (15 USC 6801): It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.

These are laws and regulations governing organizations operating in the U.S.

**Sarbanes-Oxley Act**

–

The Sarbanes-Oxley Law of 2002 (SOX) has been called the most significant new securities law since the Securities and Exchange Commission was created in 1934. SOX places substantial additional responsibilities on officers and directors of public companies and imposes significant criminal penalties on chief executive officers (CEOs), chief financial officers (CFOs), and others who violate its provisions.

–

Which statement best describes the management component of an ISS risk and vulnerability assessment? IT MAY CONSIST OF STAFF INBERVIEWS AND DOCUMENT REVIEW

By one definition, convergence is (Tyson, 2007) the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of the organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings.

information systems security (ISS)

ISS principles center on three basic elements: confidentiality, integrity, and availability, also called the CIA triad.

**Social Engineering** Someone convinces a user to share his credentials to get on the network

**Direct Hacking** Someone goes after a system, by directly accessing it via normal channels or by exploiting a vulnerability.

**Malware** Someone attacks a system by installing software on it, either with the user's knowledge (usually hidden in other software of e-mail) or automatically, without the user's knowledge

Social engineering is the manipulation of people to get them to do something that weakens the security of the network. One of the ways criminals use social engineering is to convince people to give up their user IDs and passwords.

In a direct hacking attack, a hacker works with tools under his control to gain access to the network.

**Malware**

–

One of the most insidious mechanisms hackers use today to attack systems is malware. Malware—viruses, worms, spyware, rootkits, Trojan horses, etc.—is designed to give the cybercriminal or hacker control of the computer on which it is installed. Malware often circumvents preventive measures. These are among the reasons:

Someone attacks a system by installing software on it, either with or without the user’s knowledge. This is the definition of what type of communications attack? MALWARE

Which is an information security management system?

* 

ISO 27001 and 27002

What is the first job of the person charged with responsibility for an organization’s information systems security? Create an information security management system appropriate for the organization