**Final Exam Reference**

**Trojan:**

     Malware that appears to be desirable code that, when executed, can cause harm to computing systems and data.

**Correct!**

**Virus:**

          Malware that inserts itself into applications that, when executed, can cause harm to computing systems and data.

**Correct!**

**Ransomware:**

          Malware that, when executed, encrypts data to make it unusable, causing victims to have to pay for the keys to unencrypt the files.

**Correct!**

**Worm:**

         Malware that propagates on its own and can cause damage to systems and data.

* When implementing a risk management capability in an organization, which is the first activity that a cybersecurity leader should do?
  + The leader should identify and inventory relevant cybersecurity aspects of the organization
* Which of the following best define what a vulnerability is, in terms of cybersecurity risk management?
  + A weakness in a system that can be exploited and cause harm to system or system data

**Maintaining Data Confidentiality**

               Protecting information from being accessed by unauthorized parties

**Correct!**

**Maintaining Data Integrity**

           Assuring the accuracy and completeness of data over its entire lifecycle

**Correct!**

**Maintaining Data Availability**

 Ensuring information and information systems are accessible to authorized users

**Threats**

               Actor, event, or action that seeks, identifies, or exploits a vulnerability that results in derogatory outcomes

**Vulnerability**

               A weakness in a system that can be exploited and cause harm to system or system data

**Risk**

         The culmination of exploiting actions and exploitable system weaknesses

Diagram, schematic

Description automatically generated

Risks are always remeasured as you go through the security lifecycle

* All risks are remeasured even the ones that are accepted and mitigated

**About risk and risk management:**

* When identifying risks, you look at relevant threats and vulnerabilities in your organization
* Risk is mitigated, transferred, or accepted
* Risk management means continually assessing organizational risk and then determining how best to act on the risk

**Threats**

**Black Hat**

               Criminals who have only malicious intent to break into computer systems

**Grey Hat**

               Generally, hobbyists who explore weaknesses in systems and will often inform an organization of a discovered weakness!

**White Hat**

               An ethical penetration tester who organizations hire to find weaknesses and exploits

**Social engineering:**

* a strategy where criminals rely on human social norms and trust to get information

* Insider
* Man-in-the-middle
* Reconnaissance
* DDoS

***Aspects of an organization that are considered as part of inventorying the environment ("establishing the context") in the beginning of risk management***

* Regulations that the organization must comply with
* Third parties that they share data with
* Whether they have a complex IT environment

**Risk management lifecycle**

* Identify and Inventory the Environment
* Identify Threats and Vulnerabilities and Controls
* Identify and Measure Risk
* Prioritize Risk
* Identify Control Objectives to Mitigate Priority RIsks
* Apply Controls
* Measure Efficacy of the Controls
* Repeat

**Vulnerability:**

* Identity
* Authorization
* Access Control
* Data Storage and Transmission
* System Configuration (hardware, OS, infrastructure)
* Coding (applications, services)
* Nonrepudiation
* Policies
* Physical environment

**Vulnerability types:**

Cross site scripting

Injection

**FISMA**

               Standard that federal agencies, or those that participate in federal programs, must comply with

**PCI-DSS**

         Standard for security controls for organizations that process, store, or transmit credit card data

**SOX 404**

       Standard for controls that ensures financial statement accuracy for publicly traded organizations

**HIPAA**

         Standard for covered healthcare entities to protect the C-I-A of electronic patient healthcare information

**Types of Control:**

***Physical***: an implemented capability to provide protections for actual physical environments.

***Technical***: an implemented capability that enforces the behavior and activities to some extent or level of effectiveness.

***Administrative***: policies, processes, or procedures that define broad range of behavior and activities that need to be done to meet a control objective.

**Reconnaissance**

               An attacker is gathering information in multiple ways to plan an attack approach.

**Scanning**

               An attacker is actively interacting with elements of the intended target as part of executing the attack plan

**Gaining Access**

               An attacker is exploiting a vulnerability and is looking to get a foothold into the target's environment

**Maintaining Access**

               An attacker is performing multiple steps to avoid detection, improve ability to operate in the target's environment, set up methods to continue its exploit

**Clearing Tracks**

               An attacker is using methods to discourage the target's forensics capability which could expose the attacker's methods

**Private**

               Resources are provided for the sole use of a single subscriber

**Correct!**

**Public**

               Resources are available to multiple subscribers

**Correct!**

**Hybrid**

               A subscriber may be given a mix of dedicated resources and shared resources

Responsibilities kept by cloud customer:

**Software as a Service**

               Lowest

**Infrastructure as a Service**

               Highest

**Platform as a Service**

Text

Description automatically generated with low confidenceTable

Description automatically generated               Middle

When cybersecurity professionals consider security in the cloud/cloud computing or with Internet of Things technology, they find that they must often deal with an unfamiliar set of controls that are different than typical controls that meet their control objectives.   They have same control objectives as traditional security system.

**Challenges in cloud:**

1. Data and System Visibility
2. System Configuration and Hardening
3. Access controls
4. Extension of controls and resource issue
5. Advanced threats to cloud app providers
6. Compliance

**Cyber Kill Chain**

The cyber kill chain provides discrete phases of an attacker's methods to provide precise approaches for controls to work

**IoT needs:**

Common data standards

Common communication platforms

Common security standards

Common connectivity standards

Application Integration standard and capabilities

IoT has the same Threat, vulnerability and risk analysis as a traditional information security system

* risk prioritization
* risk management lifecycle, control objectives
* **different controls have to be considered: (New)**
* The controls available / not available from “control catalog”​
* The methods of control assurance will change​
* Risk tolerance may have to be re-examined

**Challenges of IoT**

1. Constant communication
2. Need for embedded authentication
3. Constant update of access control
4. Ensuring confidentiality
5. Switch from “customer info” to availability/integrity

**Challenges of Privacy in IoT**

1. Data sharing is essential for IoT to function
2. Data unrelated to the function is collected and not needed