**Weekly Assignment 9**

Download the Assignment9FISMA guidelines from Canvas.

Review the guidelines and then answer the following questions:

1. What is the purpose of this document? Who or what would need to follow these guidelines?

The purpose of the US-CERT Federal Incident Notification Guidelines is to provide detailed procedures and requirements for reporting cybersecurity incidents to the National Cybersecurity and Communications Integration Center (NCCIC) and the United States Computer Emergency Readiness Team (US-CERT). These guidelines are intended to help ensure timely, consistent, and accurate reporting of incidents that affect the integrity, confidentiality, or availability of federal information systems. The main objectives of the document include:

* **Improving Incident Response**: By providing a clear framework for incident reporting, the guidelines aim to expedite the notification and response process.
* **Enhancing Situational Awareness**: The guidelines promote better information sharing and situational awareness across federal agencies and other stakeholders.
* **Supporting Compliance**: They help federal agencies comply with the Federal Information Security Modernization Act (FISMA) requirements regarding incident reporting.
* **Facilitating Coordination**: The document aids in the coordination between different entities involved in cybersecurity, ensuring a unified approach to handling incidents.

 **Mandatory for**:

* **Federal Executive Branch Civilian Agencies**: All civilian agencies within the federal Executive Branch are required to follow these guidelines. This includes reporting incidents involving their information and information systems, regardless of whether these systems are managed by the agency itself, a contractor, or another source.

 **Voluntary for**:

* **State, Local, Tribal, and Territorial Government Entities**: These entities are encouraged to follow the guidelines to improve incident reporting and response but are not mandated by FISMA.
* **Information Sharing and Analysis Organizations (ISAOs)**: Private-sector organizations that have established agreements to share and analyze information related to cybersecurity are encouraged to follow the guidelines.
* **Foreign, Commercial, and Private-Sector Organizations**: These organizations can adopt the guidelines on a voluntary basis to enhance their cybersecurity practices and reporting capabilities.
* **Other Non-Federal Entities**: Any other organizations that wish to align their incident reporting practices with federal standards can voluntarily follow these guidelines.

1. What is the purpose of the attack vectors taxonomy?

The purpose of the attack vectors taxonomy in the US-CERT Federal Incident Notification Guidelines is to provide a standardized classification system for identifying and describing the methods used in cyber attacks. This taxonomy helps ensure consistent communication and understanding of incidents across various entities involved in cybersecurity. Specifically, the taxonomy serves the following purposes:

**1. Standardization of Incident Reporting**

By adopting a common set of terms and relationships between those terms, the attack vectors taxonomy ensures that all elements of the federal government and supported organizations use the same language when reporting cybersecurity incidents. This consistency is crucial for clear and effective communication.

**2. Improved Incident Analysis**

A standardized taxonomy allows for more efficient and accurate analysis of incidents. When incidents are reported using a common framework, it is easier for analysts to identify patterns, understand the nature of attacks, and develop appropriate responses. This aids in the overall understanding of cybersecurity threats and vulnerabilities.

**3. Enhanced Situational Awareness**

Using a common taxonomy enables better information sharing and situational awareness. When all entities describe incidents in the same way, it becomes easier to aggregate data, compare incidents, and recognize trends. This helps in maintaining a comprehensive view of the cybersecurity landscape and in making informed decisions.

**4. Facilitation of Coordinated Responses**

A unified approach to describing attack vectors helps in coordinating responses to incidents. Different entities, such as federal agencies, state and local governments, and private-sector organizations, can more effectively collaborate and coordinate their efforts when they have a shared understanding of the attack methods.

**5. Clarity in Communication**

The taxonomy helps in clearly communicating the specifics of an attack. Different stakeholders, including incident responders, managers, and policymakers, can quickly grasp the nature of an incident based on the standardized categories. This clarity is essential for timely and effective decision-making.

**Summary of Attack Vectors in the Taxonomy**

The attack vectors taxonomy includes a high-level set of categories, each with a description and example to aid in identification and reporting:

* **Unknown**: Cause of the attack is unidentified.
* **Attrition**: Brute force methods to compromise, degrade, or destroy systems.
* **Web**: Attacks executed from a website or web-based application.
* **Email/Phishing**: Attacks executed via email messages or attachments.
* **External/Removable Media**: Attacks executed from removable media or peripheral devices.
* **Impersonation/Spoofing**: Replacement of legitimate content/services with malicious substitutes.
* **Improper Usage**: Incidents resulting from violations of acceptable usage policies by authorized users.
* **Loss or Theft of Equipment**: Loss or theft of computing devices or media used by the organization.
* **Other**: Attack methods that do not fit into any other vector.

In conclusion, the attack vectors taxonomy is a critical component of the US-CERT Federal Incident Notification Guidelines, facilitating standardized, clear, and effective incident reporting and response.

1. Who decides what level a breach should be considered?

**1. Impacted Agency's Responsibility**

* **Primary Decision-Maker**: The impacted federal agency is ultimately responsible for determining the severity level of a breach. This includes evaluating the impact on their information systems and categorizing the incident based on the guidelines provided.
* **Criteria for Major Incidents**: Agencies use criteria set out in the most recent Office of Management and Budget (OMB) guidance to determine whether an incident qualifies as a major incident. Major incidents must be reported to Congress within 7 days of identification.
* **Consultation**: Agencies may consult with US-CERT to help determine the severity level, especially when designating an incident as major.

**2. NCCIC/US-CERT Role**

* **Severity Assessment**: NCCIC/US-CERT analyzes reported incidents using the NCCIC Cyber Incident Scoring System (NCISS). This system assesses various incident attributes, including functional impact, information impact, recoverability, observed activity, and other factors.
* **Risk Rating**: Within one hour of receiving a report, NCCIC/US-CERT provides the agency with a tracking number and a risk rating based on the NCISS.
* **Suggestions for Major Incidents**: If NCCIC/US-CERT determines that an incident meets the criteria for High (Orange) on the Cyber Incident Severity Schema, it will suggest to the agency that the incident be designated as a major incident.

**3. FISMA and OMB Guidelines**

* **Framework for Decision**: The Federal Information Security Modernization Act (FISMA) and OMB guidelines provide the framework and specific criteria that agencies must use to assess and report incidents. These guidelines ensure consistency and compliance with federal standards.

**Process for Determining Severity Level**

1. **Initial Identification**: The agency’s top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or IT department identifies and assesses the incident.
2. **Initial Reporting**: The agency reports the incident to NCCIC/US-CERT with the best available information, including an initial assessment of the impact.
3. **NCISS Evaluation**: NCCIC/US-CERT evaluates the incident using the NCISS, considering factors such as functional impact, information impact, recoverability, and others.
4. **Risk Rating**: NCCIC/US-CERT assigns a risk rating and provides feedback to the agency.
5. **Major Incident Determination**: For significant incidents, the agency determines whether it qualifies as a major incident based on OMB criteria and may consult with NCCIC/US-CERT for guidance.
6. What federal governing body must be notified when there is a big incident?

 **Congress**:

* **Major Incidents**: FISMA requires federal agencies to report major incidents to Congress within 7 days of identification. This ensures that significant cybersecurity events are promptly communicated to legislative oversight bodies for transparency and accountability.
* **OMB Criteria**: Agencies must use criteria set out in the most recent OMB guidance to determine if an incident qualifies as a major incident.

 **Office of Management and Budget (OMB)**:

* **Incident Reporting Framework**: The OMB provides the guidelines and criteria that agencies must follow to classify and report incidents. This includes defining what constitutes a major incident.

 **NCCIC/US-CERT**:

* **Incident Reporting**: Agencies must report information security incidents, including those potentially compromising the confidentiality, integrity, or availability of federal information systems, to the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) within one hour of being identified.
* **Coordination and Support**: NCCIC/US-CERT helps in assessing the severity of incidents and may suggest classifying certain high-severity incidents as major.

When you are finished upload this document into Canvas for your submission.