Professional Certificate in Preventing Insider Threats

Insider Threat Legal and Ethical Considerations

Acceptable Use Policy (AUP): A set of rules that outlines how an information system or network can be used. It is designed to minimize the risk of insider threats by defining appropriate and inappropriate behavior for employees and contractors.

Adversary: An individual or group that seeks to harm an organization by exploiting its people, processes, or technology. Insider threats are often considered adversaries because they have authorized access to an organization's systems and data.

Background Check: A process of investigating an individual's past to determine their suitability for employment or access to sensitive information. Background checks can help prevent insider threats by identifying individuals with a history of malicious behavior or criminal activity.

Behavioral Analytics: The use of data and algorithms to identify patterns of behavior that may indicate an insider threat. Behavioral analytics can help organizations detect anomalous activity, such as unusual access to sensitive data or unauthorized system changes, that may indicate a potential insider threat.

Compliance: Adherence to laws, regulations, and policies that govern the protection of sensitive information. Compliance is an important consideration in preventing insider threats, as failure to comply with regulations and policies can result in legal and financial penalties.

Data Loss Prevention (DLP): A set of technologies and practices designed to prevent the unauthorized disclosure of sensitive information. DLP can help prevent insider threats by detecting and preventing the exfiltration of sensitive data through email, web uploads, and other channels.

Due Diligence: The process of investigating and evaluating the risks associated with a particular action or decision. Due diligence is an important consideration in preventing insider threats, as it can help organizations identify potential risks and take steps to mitigate them.

Ethics: A set of moral principles that govern behavior. Ethical considerations are an important part of preventing insider threats, as they help ensure that employees and contractors act in the best interests of the organization and its stakeholders.

Exfiltration: The unauthorized transfer of sensitive information from an organization's systems or network. Exfiltration is a common tactic used by insider threats to steal sensitive data or intellectual property.

Incident Response: The process of responding to a security incident, such as a data breach or cyber attack. Incident response is an important part of preventing insider threats, as it can help organizations detect and respond to potential threats in a timely and effective manner.

Insider Threat: An individual or group with authorized access to an organization's systems or data who uses

that access to harm the organization. Insider threats can take many forms, including malicious insiders, negligent insiders, and compromised insiders.

Legal Considerations: The various laws and regulations that govern the protection of sensitive information. Legal considerations are an important part of preventing insider threats, as failure to comply with these laws and regulations can result in legal and financial penalties.

Malicious Insider: An individual with authorized access to an organization's systems or data who uses that access to intentionally harm the organization. Malicious insiders may steal sensitive data, disrupt operations, or engage in other harmful activities.

Negligent Insider: An individual with authorized access to an organization's systems or data who inadvertently harms the organization through carelessness or lack of awareness. Negligent insiders may inadvertently expose sensitive data, fall for phishing attacks, or engage in other risky behaviors.

Policy: A set of rules and guidelines that govern behavior within an organization. Policies are an important part of preventing insider threats, as they help ensure that employees and contractors understand what behavior is and is not acceptable.

Privileged Access: The highest level of access to an organization's systems or data. Privileged access is typically reserved for a small number of individuals, such as system administrators or senior executives. Insider threats who have privileged access can cause significant harm to an organization.

Risk: The potential for harm or loss. Risk is an inherent part of any organization, and managing risk is an important part of preventing insider threats.

Security Awareness Training: Training designed to educate employees and contractors about the risks associated with information security and how to mitigate those risks. Security awareness training is an important part of preventing insider threats, as it can help employees and contractors understand the importance of information security and how to avoid risky behaviors.

Two-Factor Authentication (2FA): A security measure that requires users to provide two forms of authentication before gaining access to a system or network. 2FA can help prevent insider threats by adding an additional layer