Roles and Responsibilities Transcript

Welcome to this video presentation (slides with voiceover), on roles and responsibilities. A security role is the part an individual plays in the overall scheme of security implementation and administration within an organisation. Ownership is the formal assignment of responsibility to an individual or group; a company document can define owners, but cannot enforce ownership!

We will begin the lecture by looking at the different roles within an organisation and the responsibilities each role has. Firstly, the Senior Manager, this is the organisational owner whose role is assigned to the person who is ultimately responsible for the security maintained by an organisation and the most concerned for the protection of its assets. The Senior Manager signs off all the policy issues and endorses the security policy indicating accepted ownership of the implemented security within the organisation.
The Security Professional, information security officer or computer incident response team (CIRT) role, is assigned to a trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management. They have functional responsibility for security, writing the security policy and implementing it. This role can be assigned to a team and not just an individual.
The Data Owner is a role assigned to the person responsible for classifying information for placement and protection within the security solution. This tends to be a high-level manager who is ultimately responsible for data protection and usually delegates the responsibility of the actual data management tasks to a data custodian.

The Data Custodian role is assigned to the user who is responsible for the task of implementing the prescribed protection defined by the security policy and senior management. This person performs all the activities needed for adequate protection for the CIA Triad of data, as well as fulfilling the requirements and responsibilities delegated from senior management. These activities might include performing and testing backups, validating data integrity, deploying security solutions, and managing data storage based on classification. The User, end user, or operator role is assigned to any person who has access to the secured system. The user's access is in line with their work tasks and limited to only the amount of access needed to perform their tasks. They are responsible for understanding and upholding the security policy of an organisation by following prescribed operational procedures within defined security parameters. Induction and continuous training of the users is paramount.
The Auditor is responsible for reviewing and verifying the security policy is correctly implemented and the security solutions are adequate. This role may be assigned to a security professional or a trained user who produces compliance and effectiveness reports that are reviewed by senior management. Any issues found in these reports are transformed into new directives assigned by the senior manager to security professionals or data custodians.

With regard to roles and responsibilities, security regulators need to see the controls of the security measures compliance is upheld. Management need to be aware of any problems that might occur. It is essential that no shortcuts are taken as this is breaking the law and a lack of compliance can result in added risks, fines and offences.

Roles and Responsibilities
Transcript

An Acceptable Use Policy (AUP) should be signed to the users and it defines acceptable behaviours and activities, and highlights any constraints, rules and limitations of use. It can be linked to roles and responsibilities and failure to comply with these may result in serious consequences.
Privacy policy or notice is a best practice policy that is required by law and is now imposed by GDPR regulations that we looked
at last week. These regulations are when collecting and processing personal information. It is a legal agreement detailing how information is used within the organisation.

Principle of Least Privilege, is where employees have the least access privileges that they require to perform their business function.
Separation of Duties (SoD), is requiring more than one person to complete a task to prevent fraudulent activities as one person does not have all the power.
Mandatory vacation/job rotation is for persons in highly sensitive roles where it is mandatory that they take sufficient holidays to allow for a full auditing of their systems to detect any malicious activity. Job rotation is where employees rotate their roles in order to reduce malicious activity fraud and certain roles have a fixed time limit to them. Cross training is not the same as rotating roles, it is where employees are trained to perform more than one role, and has added benefit for business continuity and means that there are trained employees on hand to take over whenever necessary. Duel Control is where two people work together on a particular task to complete it in order to achieve a high level of security for critical material and operations. All access and actions require the presence and action for two authorised people. M of N requirement is where multiple people work on a task to complete it.

As we have seen previously, responsibility and accountability are of the utmost importance. Organisational security policies are everyone's responsibility. Compliance with security requirements designated by the organisation is essential. Awareness of suspicious activity, security violation and concerns is the responsibility of everyone within the organisation.

Take a break and reflect on what we have learned so far before moving on to the next task for the week.