**Team Leader**

This individual is responsible for the team’s actions. He or she is usually a senior manager with expertise in security. However, some CIRTs identify the first team member that arrives on the scene as the team leader. This person takes charge of the incident and directs other members' activities.

**Information Security Members**

These individuals could be experts on boundary protection. This includes firewalls and routers on the edge of the network. They are able to identify the source of breaches and recommend solutions. These members could also be experts in intrusion detection systems (IDSs) and other systems that include audit logs and audit trails.

**Network Administrators**

These individuals understand the details of a network. They understand what systems are connected and how they are connected. They also understand what systems are accessible from the Internet. They can differentiate normal traffic flow from abnormal traffic.

**Physical Security Personnel**

Attackers can be social engineers and might be on company property. Therefore, physical security personnel need to be represented on the team. They know which physical security controls are used and where they are used. They also know the different types of surveillance methods, such as recording cameras, used within the organization.

**Legal Personnel**

These individuals provide advice on the organization’s legal responsibilities and legal remedies. They can provide advice before, during, and after an incident. The legal team understands the legal actions that are possible against the attackers and the requirements necessary to pursue legal actions.

**Human Resources (HR)**

If the attack originated from an employee, HR needs to be involved. HR understands the policies and enforcement methods that are available. For example, if an employee violates the acceptable use policy (AUP), the first offense may result in a formal written warning. A second or third offense may result in termination. HR personnel would know if the employee had been previously warned.

**Public Relations (PR)**

These individuals become the face of the organization if the incident goes public. They help to present an image of resolve, even if everything is not quite under control. If PR representatives aren’t used, there is the risk of team members expressing frustration or confusion about the attack. This can present a poor image to customers, vendors, and stockholders of the organization.