Threat Consequence	**Threat Action (attack)**
(Unauthorized) Disclosure	A. "Exposure": A threat action whereby sensitive data is directly released to an unauthorized entity. B. "Interception": A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. C. "Inference": A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. D. "Intrusion": A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception	A. "Masquerade": A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. B. "Falsification": A threat action whereby false data deceives an authorized entity. C. "Repudiation": A threat action whereby an entity deceives another by falsely denying responsibility for an act.
Disruption	A. "Incapacitation": A threat action that prevents or interrupts system operation by disabling a system component. B. "Corruption": A threat action that undesirably alters system operation by adversely modifying system functions or data. C. "Obstruction": A threat action that interrupts delivery of system services by hindering system operations.
Usurpation	A. "Misappropriation": A threat action whereby an entity assumes unauthorized logical or physical control of a system resource. B. "Misuse": A threat action that causes a system component to perform a function or service that is detrimental to system security.

Threat consequences and threat actions from RFC 2828, *Internet Security Glossary.*