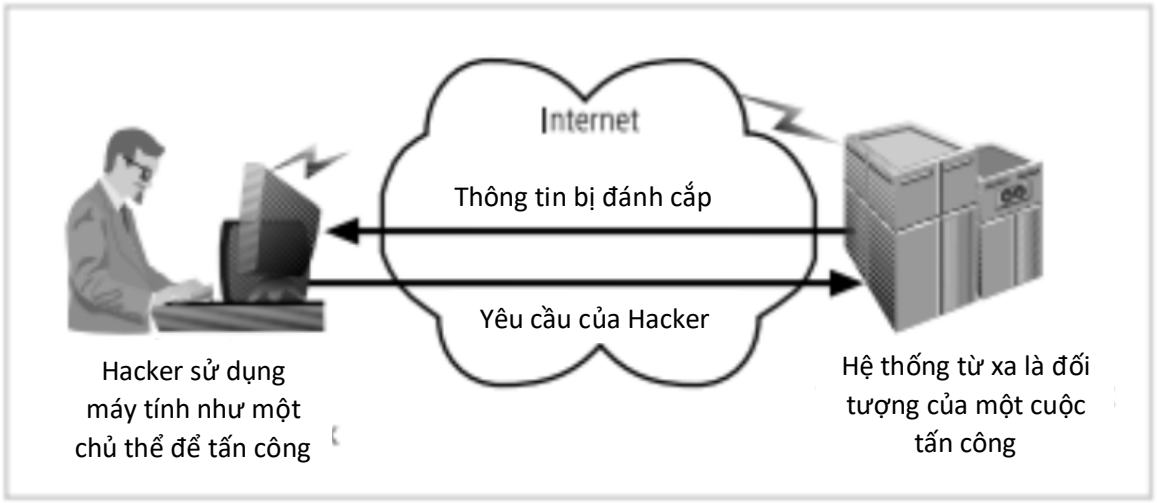
- ***Exposure***: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.
- ***Lộ***: Tình trạng hoặc trạng thái bị lộ. Trong bảo mật thông tin, thông tin bị lộ khi có một lỗ hổng mà tin tặc đã biết.
- ***Loss***: A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.
- ***Mất mát***: Là khi tài sản thông tin bị thiệt hại hoặc bị sửa đổi hoặc tiết lộ trái phép hoặc ngoài ý muốn. Khi thông tin của một tổ chức bị đánh cắp, tổ chức đó coi như đã phá sản.
- ***Protection profile*** or ***security posture***: The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term security program, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.
- ***Hồ sơ bảo vệ*** hoặc ***tình trạng bảo mật***: Toàn bộ tập hợp các biện pháp kiểm soát và bảo vệ, bao gồm chính sách, giáo dục, đào tạo, nhận thức, và công nghệ mà tổ chức triển khai (hoặc không thực hiện) để bảo vệ tài sản. Các thuật ngữ này đôi khi được sử dụng thay thế cho thuật ngữ chương trình bảo mật, mặc dù chương trình bảo mật thường bao gồm các khía cạnh quản lý của bảo mật, bao gồm lập kế hoạch, nhân sự và các chương trình cấp dưới.
- ***Risk***: The probability that something unwanted will happen.
- ***Rủi ro***: Khả năng xảy ra điều không mong muốn.

Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept.

Các tổ chức phải giảm thiểu rủi ro để phù hợp với ***khẩu vị rủi ro*** (Khẩu vị rủi ro là mức độ rủi ro mà một tổ chức hay cá nhân (các nhà đầu tư hay thương nhân) sẵn sàng chấp nhận để theo đuổi các mục tiêu tài chính của mình, trước khi hành động được xem là cần thiết để giảm thiểu tối đa rủi ro.) của họ — số lượng và bản chất của rủi ro mà tổ chức sẵn sàng chấp nhận.

- ***Subjects*** and ***objects***: A computer can be either the **subject** of an attack—an agent entity used to conduct the attack—or the object of an attack—the target entity, as shown in Figure 1-4. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).
- ***Chủ thể*** và ***đối tượng***: Một máy tính có thể là đối tượng của một cuộc tấn công - một thực thể tác nhân được sử dụng để thực hiện cuộc tấn công - hoặc đối tượng của một cuộc tấn công - thực thể mục tiêu, như trong Hình 1-4. Một máy tính có thể vừa là chủ thể vừa là đối tượng của một cuộc tấn công, ví dụ, khi nó bị xâm nhập bởi một cuộc tấn công (đối tượng), và sau đó được sử dụng để tấn công các hệ thống khác (chủ thể).



Hình 1.4 Máy tính vừa là chủ thể và đối tượng của một cuộc tấn công

- ***Threat*:** A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.
- ***Mối đe doạ***: Một loại đồ vật, con người hoặc các thực thể gây nguy hiểm cho tài sản. Các mối đe dọa luôn hiện hữu và có thể có mục đích hoặc không có định hướng. Ví dụ, tin tặc cố tình đe dọa các hệ thống thông tin không được bảo vệ, trong khi các cơn bão nghiêm trọng vô tình đe dọa các tòa nhà và những thứ bên trong.
- ***Threat agent*:** The specific instance or a component of a threat. For example, all hackers in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.
- ***Tác nhân đe dọa**:* Là một đối tượng cụ thể hoặc một thành phần của mối đe dọa. Ví dụ, tất cả các tin tặc trên thế giới đều là mối đe dọa chung, trong khi Kevin Mitnick, người bị kết án vì hack vào hệ thống điện thoại, là một tác nhân đe dọa cụ thể. Tương tự như vậy, sét đánh, mưa đá hoặc lốc xoáy là một tác nhân đe dọa là một phần của mối đe dọa - các cơn bão nghiêm trọng.
- ***Vulnerability*:** A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some **well-known vulnerabilities** have been examined, documented, and published; others remain latent (or undiscovered).
- ***Tính dễ bị tấn công***: Một điểm yếu hoặc lỗi trong hệ thống hoặc cơ chế bảo vệ khiến nó bị tấn công hoặc gây thiệt hại. Một số ví dụ về lỗ hổng bảo mật là lỗ hổng trong gói phần mềm, cổng hệ thống không được bảo vệ và cửa không khóa. Một số **lỗ hổng bảo mật nổi tiếng** đã được kiểm tra, ghi lại và được phát hành; những thứ khác vẫn tiềm ẩn (hoặc chưa được khám phá).