Information Security and Privacy

> Prerequisites: Information Systems

> Unless otherwise specified, all quotes in this document are based on chapters 4.1 and 4.5 of *Intro to Information Systems (5e)*, by Rainer.

Security refers to protection from "unauthorized access, use, disclosure, disruption, modification, or destruction" of information resources.

Privacy is "the right to be left alone and to be free of unreasonable personal intrusion".

Threats, or dangers, to information resource security and privacy generally include intentional or unintentional actions like hacks and attacks, hardware and software failures, natural disasters, and human mistakes and negligence.

To maximize information security and privacy, technology administrators must take proactive measures such as conducting periodic security audits and creating disaster recovery procedures.

Ultimately, information security and privacy practitioners rely on principles of risk management and mitigation, which involve the intentional assumption of a certain level and nature of risk.

Threats

This data visualization identifies some of the biggest data breaches.

What notable hacks have you seen in the news lately?

For more threats, including malware, see the notes on Software Ethics.

Controls

Physical Controls

Physical controls "prevent unauthorized individuals from gaining access", e.g. locks, walls, guards, alarm systems, login attempt limiting, etc.

Access Controls

Access controls "restrict unauthorized individuals' (access to and) use of information resources".

Authentication

Authentication is "a process which determines the identity of the person requesting access".

Multi-Factor Authentication (MFA), or two-step authentication, is "a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in, ... they will be

prompted for their user name and password (the first factor — what they know), as well as for an authentication code from their ... MFA device (the second factor — what they have). Taken together, these multiple factors provide increased security... (Amazon).

Protect your accounts with MFA:

- https://support.google.com/accounts/answer/1066447?hl=en
- https://www.facebook.com/help/148233965247823
- https://help.twitter.com/en/managing-your-account/two-factor-authentication
- https://www.dropbox.com/en/help/363
- https://get.slack.help/hc/en-us/articles/204509068-Set-up-two-factor-authentication
- https://aws.amazon.com/iam/details/mfa/

Authorization

Authorization "determines (the permissible) actions, rights, or privileges (of an individual who has verified his/her) identity".

The **Principle of Least Privilege** calls for granting a privilege to an individual only if the individual's need is justified. In other words, start from a situation in which no one has any privileges, and add them one-by-one as necessary. Contrast this against an open permission structure by which everyone starts with all privileges and they are revoked one-by-one as necessary.

Communications Controls

Firewalls

A **firewall** "prevents unauthorized users from accessing private networks ... or certain parts of private networks".

Encryption

Public Key Encryption

A **key pair** consists of a **public key** file often named `id_rsa.pub` which may be shared or otherwise transmitted over computer networks, as well as a **private key** file often named `id_rsa` which should NEVER be shared or otherwise transmitted over computer networks.

Here are instructions for how to generate a public/private key pair.