Security policies (Build B 2.7)

EUCIP CORE SYLLABUS 3.1

These are the main types of security policies used by organisations:

- **Human security** – For many organisations, security begins at the **physical level** and controls are put in place to ensure that only authorised users access the buildings, rooms, computers and the files where data are stored. This is usually achieved by access control systems using both security badges and badge readers, to simply having locks or doors to allow entry only to authorised people.
- Unfortunately, a main concern of many organisations is how employees control their own passwords and security as in many cases the human element is the weakest in the system. For that reason, a common security practice in organisation is to limit what information employees can print.
- **Operating System Security** – All servers, routers and other active network equipment is in locked cabinets or purpose-built server rooms and access is provided only to IS (Information Security) employees. There are strict guidelines for passwords and remote access to vital servers is strictly limited to authorised users. The IS teams patch management policy ensures that all servers carry the latest operating system patches and that all desktop PCs and workstations are adequately protected against any malicious attacks. The installation of anti-virus software and its regular updating including protection against malware and spyware is undertaken by the IS team.

Bit by Bit, *New Edition* - Copyright © EDISCO Editrice - Vietata la vendita e la diffusione

- **Network security** – Regular security audits help enforce IS controls. When an intruder breaches the network, server or storage defences, he usually has one of three goals: to look at information, to deny the company the use of data, or to damage or destroy data. Because the harm is intentional, an intruder can do more selective damage aimed at long-term harm. For this reason, it is important to keep backups or copies of data, in case a security breach results in damage or destruction of critical data. These backups are also essential in case of accidental loss of data or system failure. Another problem is related to the fact that a network based system has more access points and, therefore, a greater need to ensure each of these points is configured to only allow access to authorised users.
- **Database security** – Together with all of the security systems described above, many database systems contain inbuilt security features which, together with best practices, can define a good security policy for an organisation.

1 **After studying the previous page, cover it and try this test. You have to choose the right answer for each question.**

1. Controls at physical level include...
- **a.** the use of badges.
- **b.** special keys.
- **c.** blocking doors.
- **d.** the use of special lockers.

2. The main risk related to passwords is the fact that...
- **a.** they are too short.
- **b.** they are difficult to remember.
- **c.** employees don't keep them in a secure place.
- **d.** they are often forgotten.

3. The four main types of security policies are:
- **a.** human, operating system, network, database.
- **b.** human, hardware, network, database.
- **c.** human, operating system, network, data.
- **d.** human, operating system, encryption, data.

4. The people who have access to servers and routers are...
- **a.** all staff.
- **b.** executive officers.
- **c.** IS employees.
- **d.** IS managers.

5. As for Operating System Security, ...
- **a.** there are strict guidelines for accessing the cabinets.
- **b.** access to servers is limited to authorised people.
- **c.** employees run patches daily.
- **d.** only server data are backed up.

6. Breaches in a network are...
- **a.** unintentional.
- **b.** meant to damage or destroy data.
- **c.** meant to back up data.
- **d.** aimed at destroying hardware.

Bit by Bit, *New Edition* - Copyright © EDISCO Editrice - Vietata la vendita e la diffusione

7. Backups...
- **a.** are not used after security breaches.
- **b.** are optional.
- **c.** are useless in case of accidental loss of data.
- **d.** are essential in case of data failure.

8. Database security...
- **a.** does not use special systems.
- **b.** does not contain inbuilt security features.
- **c.** does not use best practices.
- **d.** does not provide a reliable security system.

Bit by Bit, *New Edition* - Copyright © EDISCO Editrice - Vietata la vendita e la diffusione