Assignment 1

Wajiha Batool – 19684

About IBA

The oldest business school in Pakistan is the Institute of Business Administration Karachi (IBA). It was established in 1955 with administrative and faculty assistance from the University of Pennsylvania for the first five years and the University of Southern California for the following five. Since its inception, the Institute has continually upheld a reputation as Pakistan's top business school while simultaneously expanding into new fields outside of business administration.

IBA provides degrees in business administration, accounting and finance, computer science, economics, mathematics and economics, social sciences, and liberal arts at the undergraduate level.

Graduate degrees in business administration, MBA executive, computer science, economics, Islamic banking and finance, journalism, management, data sciences, finance, and mathematics are among the graduate programs provided by the IBA.

The Institute provides Ph.D. programs in computer science, economics, and mathematics.

Vulnerabilities and threats

IBA ID card

A random person can enter in the campus using any student's ID card. This is a possible vulnerability because anyone who is not affiliated with IBA may access IBA through IBA-affiliated family members and friends. This is a type of physical attack.

Technical security action that can be taken to avoid this problem is to install facial recognition or thumb impression systems at the entrance and exit so that non-IBA-associated persons could not enter the campus.

Due to the possibility of illegal access to the campus's grounds and its facilities, this vulnerability could jeopardize the organization's capacity to maintain its confidentiality. These individuals may also pose a threat to the staff, students, and faculty members' safety.

Malicious Emails

All students of BSCS received malicious emails. Since only administrative personnel can access this email group, this was an insider attack committed by a member of staff or any intruder who got access to these private groups of the organization.

The authorized staff should keep an eye on such activities and filter such emails using content search as the outlook is a Microsoft office product that allows global and exchange administrators to closely monitor the activity of email senders.

Such emails can seriously jeopardize the organization's confidentiality because the attacker has access to some of our personal information linked to the email account. Such emails may contain dangerous links or files that can trigger phishing attempts.

Weak Passwords

As the passwords for "IBA ILS" are the users' capitalized last names, which are fairly easy to guess, one can access the private information of other users. This is a type of access control vulnerability. The main defense against most online accounts being hacked is a strong password. If modern procedures are not used, one can be employing passwords that online scammers can quickly guess in a matter of hours.

The password of this website should be set by following modern practices which include encryption as well. The users should never put themselves at risk of identity theft and extortion, therefore if they feel that their password is not secure enough, they should change it right away.

The confidentiality of the users could be seriously compromised as a result of this vulnerability. Integrity problems may result as a consequence of the hacker's ability to modify the user's personal information through this portal. As a result, social engineering attacks like pretexting may take place since the hacker can threaten the user with the disclosure of private information.

Shuttle Service

The shuttle service of IBA provides a comfortable commute to the students who have to attend classes across the campus. Although this is a remarkable service provided by IBA, there are some vulnerabilities and threats that should be addressed promptly.

1. When using the shuttle service, the student's ID card is not inspected. Today, students are picked up by the shuttle outside gate 3. Any trespasser accessing the shuttle has a good possibility of endangering security measures.
   Administrative control should be exercised to prevent this issue by establishing a rule requiring students' facial features to match those on their ID cards. The shuttle's guards and drivers need to be made aware of the dangers that could result from allowing just anyone to board the vehicle.
   This compromises the confidentiality of the organization and students as unauthorized people could access the shuttle service. Apart from that availability is also jeopardized as sometimes the rightful people don’t get enough space in the bus to travel comfortably to their destination.

2. The information regarding the shuttle timings, pickup and drop off location is publically available on the IBA website. The same problems can occur as mentioned in point 1.

Technical control should be practiced by moving this information from this public website to the student portal where the students can sign in via their credentials and can view this information.
This jeopardizes the organization's and the student's right to privacy because anyone can use the shuttle service. In addition, accessibility is threatened since the rightful passengers occasionally do not have enough room in the bus to comfortably travel to their destination.

Same Passwords for Every Website

The same credentials are used for the ERP portal, job portal, student facilitation system, and TA management system. If any security breach occurs at any of these sites, the others will be at potential risk. This is a type of access control vulnerability.

Technical control should be practiced to avoid this problem. The passwords of all of these websites should be highly distinctive from each other so that if something unfortunate occurs with any of these websites, the rest can be kept secure.

Such types of breaches can endanger the confidentiality and integrity of the organization's data. The hacker can make modifications to the hacked account and can even change the password of the account which in turn creates a huge hindrance for the account holder to access their own account.

Students coming with their drivers/ family members

Drivers and family members who come to campus to drop off their children and have stickers on their cars can freely utilize campus facilities. This can pose a physical threat to the students, staff, faculty, and on-campus resources.

To prevent such activity, technical control should be exercised. A system should be developed that would record the entrance and checkout time of a vehicle and if any vehicle takes more than 10 minutes on campus, they should be penalized while checking out.

Since an unauthorized person would be present among the pupils and could cause them physical damage, this kind of breach could jeopardize confidentiality. As someone who is not linked with the IBA could use the organization's resources, it also impedes its availability.

Conclusion

Weak data security can cause important data to be lost or stolen, resulting in a negative customer experience and reputational damage. As individuals depend more on technology, data breaches, fraud, and cyber-security threats are all growing more frequent. So, in order to prevent such issues, adequate security measures must be performed timely.