FACULTY/COLLEGE	College of Business and Economics
SCHOOL	School of Consumer Intelligence and Information Systems
DEPARTMENT	Applied Information Systems
CAMPUS(ES)	APK
MODULE NAME	Protection of Information Assets
MODULE CODE	PGD004
SEMESTER	Second
ASSESSMENT OPPORTUNITY, MONTH AND YEAR	Final Summative Assessment Opportunity 21 November 2019

ASSESSMENT DATE	21 November 2019	**SESSION**	08-30 – 11:30
ASSESSOR(S)	Dr Mpho Raborife		
MODERATOR(S)	Mr. Blessing Ogbuokiri		
DURATION	3 hours (180 min)	**TOTAL MARKS**	100

NUMBER OF PAGES OF QUESTION PAPER (Including cover page)	2

INFORMATION/INSTRUCTIONS:

- This is a TAKE-HOME assessment.
- Answer each question in a separate book.
- Read the questions carefully and answer only what is required.
- Number your answers clearly and correctly as per the question paper.
- Write neatly and legibly on both sides of the paper in the answer book, starting on the first page.

In December 2009, a major password breach occurred that led to the release of 32 million passwords. Further, the hacker posted to the Internet the full list of the 32 million passwords (with no other identifiable information). Passwords were stored in clear text in the database and were extracted through an SQL Injection vulnerability. The data provides a unique glimpse into the way that users select passwords and an opportunity to evaluate the true strength of these as a security mechanism. In the past, password studies have focused mostly on surveys. Never before has there been such a high volume of real-world passwords to examine. The Imperva Application Defense Center (ADC) analyzed the strength of the passwords. The shortness and simplicity of passwords, means many users select credentials that will make them susceptible to basic brute force password attacks. Furthermore, studies show that about one half of the users use the same (or very similar) password to all websites that require logging in. Ironically, the problem has changed very little over the past twenty years. In 1990, a study of Unix password security revealed that password selection is strikingly similar to the 32 million breached passwords. Just ten years ago, hacked Hotmail passwords showed little change. This means that the users if allowed to, will choose very weak passwords even for sites that hold their most private data. Worse, as hackers continue to rapidly adopt smarter brute force password cracking software, consumers and companies will be at greater risk. To quantify the issue, the combination of poor passwords and automated attacks means that in just 110 attempts, a hacker will typically gain access to one new account on every second or a mere 17 minutes to break into 1000 accounts. Key Findings

- About 30% of users chose passwords whose length is equal or below six characters.
- Moreover, almost 60% of users chose their passwords from a limited set of alphanumeric characters.
- Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is “123456”.

Compile a 2 page recommendation report detailing factors that need to be taken into consideration to avoid such an event taking place in the future.