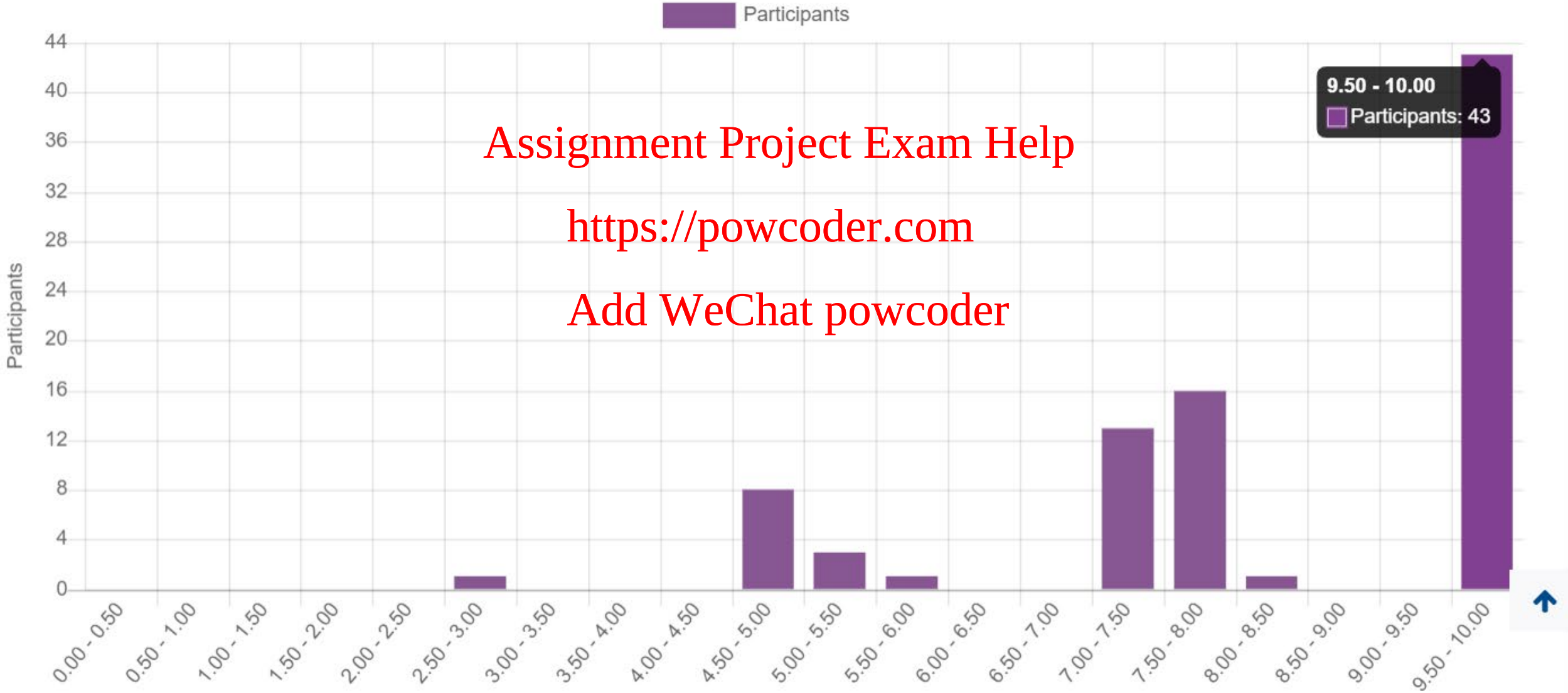
Quiz 1 - statistics

of participants: 86 / 100

average: 8.23 / 10



Consider a company for which ‘forces of nature’ is a category of threat events with a very high likelihood of occurrence. Which of the following technological practices should absolutely be avoided by this company:

1) use of cloud services

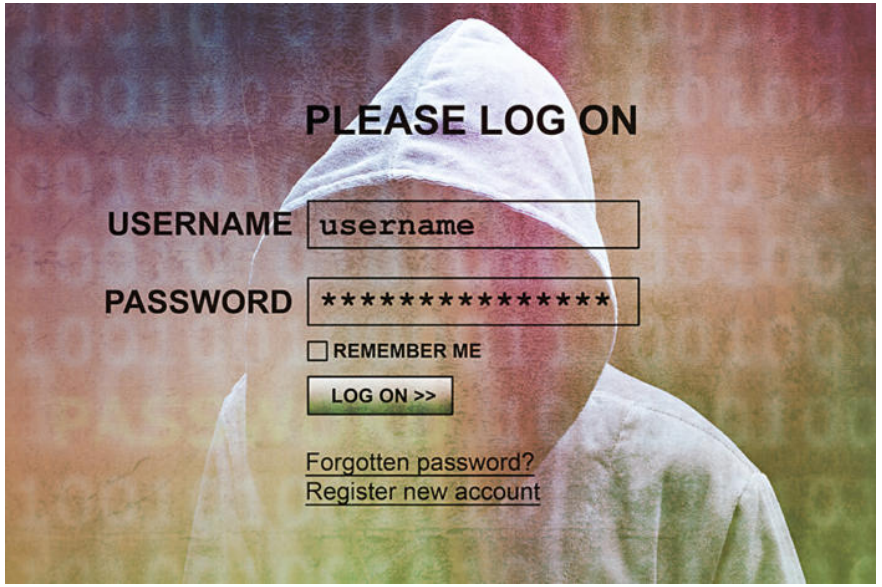
2) use of on-premise backup solutions

3) allowing BYOD

4) use of WiFi technology

A hacker known as Mallory is in possession of your PII which was leaked into the dark Web during an earlier data breach. Using this information, Malory has successfully cracked your EECS password by performing remote logging into your EECS account. In particular, already on the second log-in attempt, Malory has discovered that your EECS password is a four-digit number sequence corresponding to your day and month of birth (e.g., password is '3112' corresponding to Dec 31).
Which of the following countermeasures - as found in McCumber cube - should be improved first by EECS' security team in order to prevent similar hacks in the future:

1) technology
2) people
3) policies and practices



Alice, a YorkU employee at Student Services, uses a commonly shared printer to print out student files. Several weeks ago, she sent about 50 student files to be printed at once. During the printing process, some of the printer cabling got overheated ultimately causing fire. The fire spread from the printer room into the server room damaging a number of critical computers.

Which of the following could be named the '<u>threat agent</u>' in the above described incident:

1) employee (Alice)

Alice has not done anything wrong – printing 50 files, in an institution of YorkU size, is not much!

2) fire / forces of nature

3) hardware failure

Hardware failure is the cause (threat event) of this incident, but not the 'threat agent'

4) human error or failure

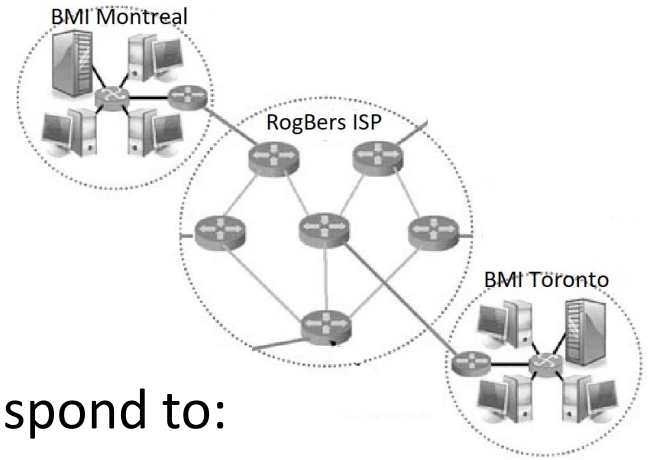
5) none of the above

MBI is a medium size software-development company with the engineering headquarters located in Toronto and the administrative headquarters located in Montreal. MBI uses the services of one single ISP named RogBers to maintain the Internet connection between the two headquarters.

A number of RogBers' routers have recently been hacked and infected with a virus. The virus causes the infected routers to drop around 50% of all routed packets, thus significantly lowering the QoS provided to RogBers' customers. As a result, it is almost impossible to conduct any zoom-conferencing between the two MBI's headquarters.

a) **From MBI's perspective**, which area of McCumber cube does this security problem correspond to. Circle everything that applies.

data at rest	data in use	data in transit
integrity	confidentiality	availability
technology	people	policies & practice



b) **From MBI's perspective**, which type of threat event does this situation correspond to:

hardware & software failure and errors

deliberate software attack

deliberate act of vandalism

act of human error or failure

none of the above