Name: Information Technology: Risk Mitigation with Data

A	Threats to Data
Destruction	Data is lost and cannot be recovered
Manipulation	Data is changed from its original form
Modification	Another way of saying manipulation
Theft	Data is stolen
Identity theft	Stolen data is used to impersonate someone

B	Consequences of Data Loss
Financial loss	If invoices are lost, income may be lost. If personal data is lost, compensation may be paid
Time	Loss of data will mean any work done to make the data will have to be done again.
Reputation	A data breach will undermine public confidence in the company which is attacked

C	Consequences of Disruption
Disruption	When a cyber-security attack interrupts the normal running of a business
Operational	A website or computer system can be stopped from working
Financial	Money can be lost through loss of customers, compensation claims and the time spent fixing the disruption
Commercial	When sales cannot be made
Safety	Disruption of the running of, eg, a power plant would pose a threat to health of the public

C	Prevention Measures
Physical	Protecting against attacks with physical means
Biometric protection	Reading data about someone's body to verify their identity. Eg fingerprint, retina scan, DNA
Locks	Securing the doors and windows to rooms with data storing machines
CCTV	Security cameras
Bolting down	Attaching computing equipment to a desk
Logical	Protecting against attacks with non-physical means
Access rights	Permissions for different users to be able to look at and edit different data
Authentication	Making sure a user is the right person by eg username and password
Two-factor	Authentication which asks for two proofs of ID, eg a password and a texted code
Anti-malware software	Software which stops viruses and other malware getting into a system
Encryption	Data is stored as an incomprehensible code until it is decrypted with a key
Secure backup	A copy of important data, preferably kept away from the original data