An online sales system of a local retail company had been hacked.
A huge amount of customer data was leaked and put on the Internet.
The affected customers filed a lawsuit against the company and requested for a compensation of HK$10 million.

These day the hackers are running rampant.
I better get Chi On to do a security check of my online store tomorrow!

(The next day)

Your online store is using an on-premise server,
yet not all security updates have been installed.
It may induce system hacking!

Oh no…what should I do?

Nowadays many companies have migrated their system from on-premise servers to cloud service,

which saves the cost of IT equipment
and can adjust the configurations and scales of the systems at any time in accordance with business needs.
The cloud service provider will also be responsible for maintaining the subscribed IT environment for you.

Generally speaking, SMEs have limited resources
and are unable to afford the enormous cost and manpower required for IT systems.
Adoption of cloud services can cater the needs of SMEs.

Sounds good!

Actually, we have uploaded some of our company files to the cloud.
Would you please also check if there is any security issue?

Let me check…
You have saved the customer order to the cloud storage,

but the security configurations have not been set properly yet!

This is a common security issue called “misconfiguration”,
which could lead to unauthorised access to your company data.
It is like leaving your front door of your home unlocked.

if it is hacked, it could result in leakage of sensitive information.

(Meanwhile)

Show time!
Let me see which online stores have security loopholes, so that I can hack into them!

…okay, this one!
Building an online store without proper security measures?
Isn’t it an easy job for me?

Wow! What should I do to protect my cloud storage?

Although the cloud service provider is responsible for protecting the cloud infrastructure,
customers should also configure the access permissions of the cloud storage properly to avoid sensitive or personal information leakage!

You should refer to the configuration manual and security guidelines from the cloud service provider when setting up your cloud service.
Once completed, check and test the related security settings.
Also, the access logs need to be reviewed regularly
for suspicious activities to ensure security.

Other than configurations, what measures could I take to ensure the security of my cloud service?

There are a few more things you could do…

First, enable the multi-factor authentication of user accounts.
Second, set up different access permissions based on the needs of various user

groups.
Third, encrypt sensitive information before uploading to the cloud.
Fourth, back up your data regularly for recovery whenever it is necessary.
Fifth, perform security risk assessment and audit for the system regularly.
You may contact your cloud service provider to check if the security configurations of the cloud service are properly set
and choose a suitable security solution for you.

Right! I better have someone to follow it up now!
It would damage our company reputation if customer information leakage happens.

Almost there…

Oh no…I failed again!

I will definitely succeed to hack into your computer next time!