6 easy steps to build your security culture

DID YOU KNOW?

2/3 of people use the **same password** everywhere[1]

Many employees **click on suspicious links** and attachments in their work inboxes

23% of workers **do not seek help from the IT team** when faced with a security concern[2]

As your workforce grows, the risk of cyberattacks also escalates. Stifle it by creating a security culture.

Instil a set of security-related norms, values, attitudes, and assumptions into your company's daily operations.

Ensure your personnel prioritise security at every moment.[3]

SECURITY DO AND DONT'S AT THREE COMPANY LEVELS

SCENARIO	✗	✓
When employees receive a suspicious email	"I'll look at it in-depth or delete it later."	"I'll let the IT team know – they can investigate it immediately."
SCENARIO	✗	✓
When managers deal with a threat	"This is a management-level concern. We don't need to involve everyone."	"Cyber security is everyone's responsibility, top to bottom."
SCENARIO	✗	✓
When company leaders discuss cyber security	"Security is someone else's area of expertise. Not mine."	"My team and I must know how we can prevent breaches."

IS YOUR SECURITY CULTURE UP TO THE MARK?

Evaluate your company with these 3 essential indicators:

Cyber security awareness

Employees across all levels grasp the significance of cyber security and their role in safeguarding it.

Proactive mindset

The organisation actively identifies and tackles potential risks before they escalate into problems.

Security integration

Staff considers security a vital part of daily tasks, fostering a collective responsibility to protect the company's assets and reputation.

Empower your workforce to be security partners with these

6 STEPS to building A SECURITY CULTURE

STEP 01

Foster security-minded leadership

Senior management must actively promote and support a strong security culture.

STEP 02

Implement strong security policies

Define, review, update and communicate security policies to all employees.

STEP 03

Establish a robust incident response plan

Effectively manage and mitigate security breaches. Leverage Singtel Cyber Security for rapid response capabilities to investigate incidents within hours.

STEP 04

Train employees to be cyber security aware

Ensure everyone knows that protecting the company's data and systems is everyone's job.

STEP 05

Establish clear reporting channels

Encourage employees to report suspicious activities, incidents, or security concerns without fear of repercussions.

STEP 06

Provide ongoing security education

Invest in regular security awareness training and provide resources to keep employees up-to-date on the latest threats and best practices.

Tell it to IT!

Train your workforce to spot and respond to cyber threats confidently and regularly. Build a robust security culture today.

Contact Us

www.singtel.com/cybersecurity

Singtel

[1] Microsoft 365, Creating a Security Culture in Your Business, 2021.
[2] Singapore Business Review, Over 6% of IT decision makers in businesses refuse to build security culture: report, 2023
[3] ICAO, Security culture, 2023