Why Should Businesses Invest in Security?

Because they experience these common

Pain Points

Panic and Frustration from not knowing what to do in an event there is a cyber attack and its potential short-term and long-term impacts

Worried that a cyber attack would jeopardize the business and its reputation, which can cause damaged customer relationships and financial loss

Invasion of privacy of valuable and sensitive information about customers who have put trust in the organization

Overwhelmed with too much information about how to prevent cyberthreats

Stressed from the lack of in-house cybersecurity skills and staffs

Fear of losing Intellectual Property, proprietary and personal information

Why Should Businesses Invest in Security?

Because they want to reap these desirable

Business Outcomes

Understand the cyber threat trends and best practices

Ensure your business continuity even after a cyber attack

Protect your reputation and instill trust in your customers

Optimally prepared (not over or under prepared) for potential cyberthreats in a **proactive** manner

Have qualified security experts providing advice and helping with security issues at the tip of your fingers

Detect if hackers have already compromised your environment

3 Action Items

1. Put a gate in place

2. Place a smart lock that's difficult to copy at the front door of your house

3. Put a "geotag" on all your valuables

3 Action Items – Email, Identity, Data

What to do	What it means in cybersecurity terms	Why?
1. Put a gate in place	Email security	• Prevent phishing attacks (the most common way account credentials are leaked)
2. Place a smart lock at the front door of your house	Identity & access management	• Prevent unauthorized login attempts • Together with Email Security, improved security for 99% of cybercrime attacks
3. Put a "geotag" on your valuables	Data security	• Prevent data theft both from external and internal actors, and both intentional and unintentional actions