Handling Objections from SME Business Managers/Owners who don't believe they need regular Vulnerability Assessments/ Health Checks

➔ **I am too small**
  - Cyber criminals are on the hunt for an open door and small businesses can present an easy target.

➔ **My data isn't valuable**
  - Really? Because all customer and employees' personnel details such as credit card, bank account, tax file and Medicare details, are valuable on the black market. Not to forget your company's own confidential information.

➔ **We are handling it**
  - How? Because traditional security protections such as firewalls, anti-virus, email and web filtering have been proven as no longer an effective deterrent in stopping successful cyber-attacks.

➔ **It's too expensive**
  - How costly is the option, small business has been known to go under within 6 months of a successful hack? The Health check will tell which specific vulnerabilities could be used to steal information.

➔ **It takes too long**
  - This where SoftGen can assist, we can run the testing and provide a report that identifies ALL vulnerabilities, prioritises each vulnerability based on its ability to provide an opportunity for a cybercriminal and just as important provide details on how to fix.

➔ **We have already had one done**
  - The level of sophistication and the frequency of attacks are increasing rapidly, any previous assessment was a snap shoot in time, things will have changed either with your IT Infrastructure or the types of cyber-attacks.

➔ **Cyber Criminals rely on Complacency**

➔ **SoftGen's goal is to make security less complexed and more affordable to the SME market** – why they are just as vulnerable as an Enterprise or government department

➔ **SoftGen provides the tools and expertise to provide a Security Health Check (Vulnerability Assessment.** Our testing is conducted based on the standards set by National Institute of Standards and Technology (NIST)

  - Identify the Systems
  - Identify and Document Internal and External Threats
  - Determine Risk and Impact
  - Analyse Controls
  - Determine the likelihood of the Risk
  - Identify and Prioritise Risk Response