Lost in Translation?

a case study
in the radical transformation of cyber hygiene controlst

SAY WHAT?

**When the message gets muddled,
it means major delays
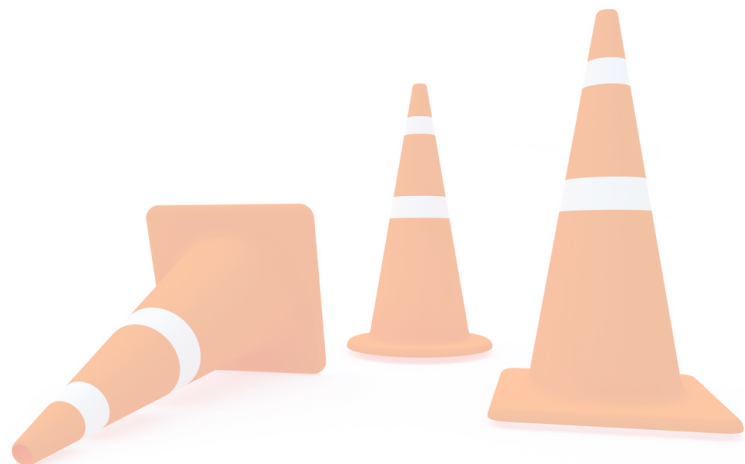in achieving cyber hygiene controls**

- How do you ensure safety standards are adhered to across all your business functions and in accordance with your company's protocols?

- How do you find and mitigate breach points in a timely manner while continuing to serve your global customer base?

- How do you ensure compliance with both Technical and Governance controls while not breaking the bank?

MEET YOUR PEER

a global telecommunications conglomerate
looking to establish a clear and concise universal language
and best practice to meet their cyber hygiene goals

- **TelCom** is leading British multinational telecommunications company that connects more than 300m mobile customers and 27m fixed broadband customers across 21 markets and 48 partner markets, and operates the largest 5G network in Europe.

- Like most Global organizations, **TelCom**'s headquarters provided cybersecurity guidelines for all their I.T. and Compliance team members and then the local or regional teams were required to execute those tasks.

- While global internal auditors periodically checked the progress over the course of the year to ensure the local team had completed these tasks, it was up to the local team to "interpret" those guidelines to the best of their understanding.
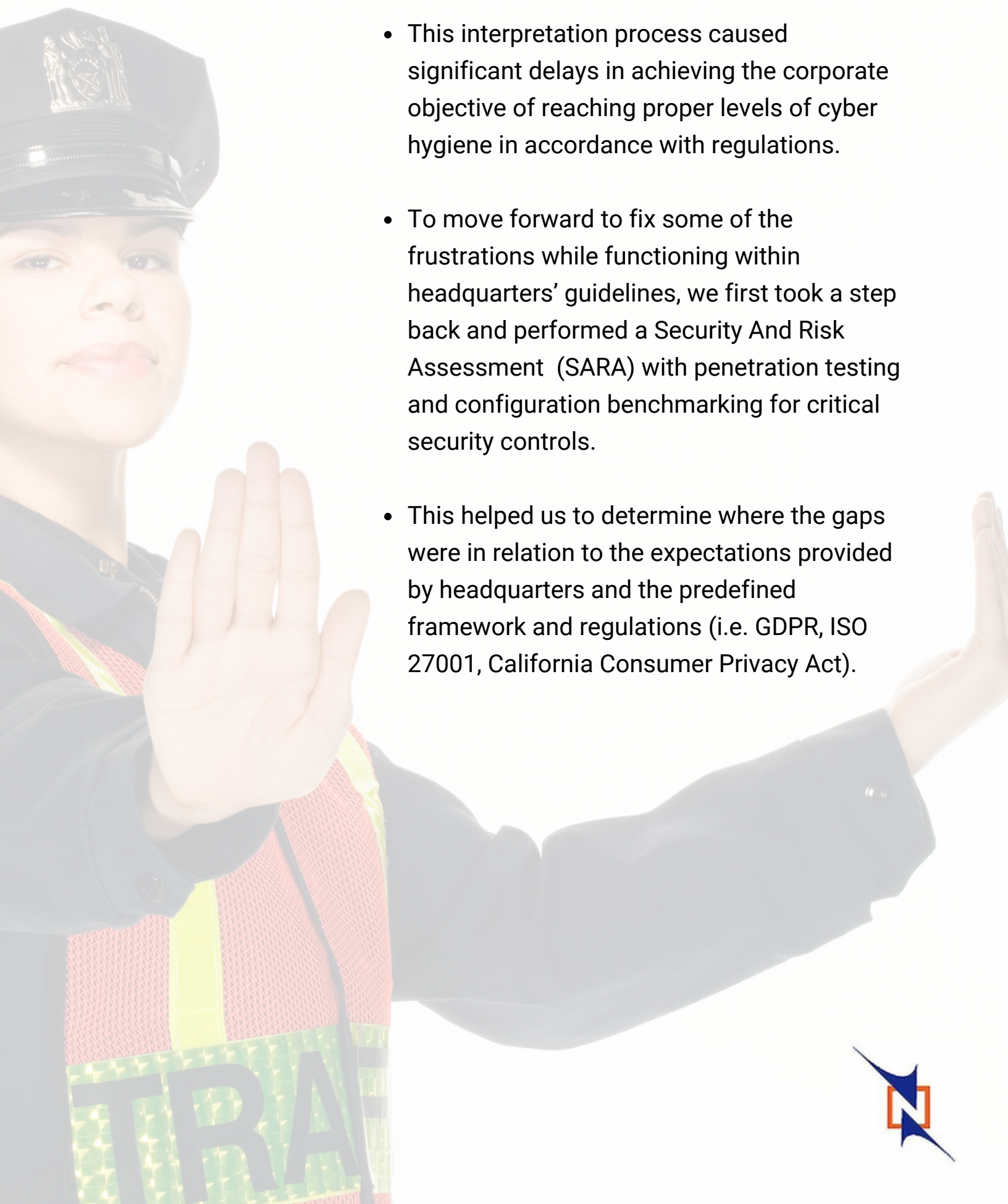
- This interpretation process caused significant delays in achieving the corporate objective of reaching proper levels of cyber hygiene in accordance with regulations.

- To move forward to fix some of the frustrations while functioning within headquarters' guidelines, we first took a step back and performed a Security And Risk Assessment (SARA) with penetration testing and configuration benchmarking for critical security controls.

- This helped us to determine where the gaps were in relation to the expectations provided by headquarters and the predefined framework and regulations (i.e. GDPR, ISO 27001, California Consumer Privacy Act).

Results You Can See

In **TelCom**'s situation we were able to locate weaknesses in parts of their cyber infrastructure that weren't currently being tested – all because SARA "saw" across their extensive business systems and alerted us to the similar weaknesses across their international platforms.

Our penetration test process also provided **TelCom** with a comprehensive list of breach points across their system and a step-by-step plan on how to mitigate each hazard across functions.

TelCom was successful in identifying, addressing, and preventing each possible event leading to a safer, more secure infrastructure.

By providing **TelCom** with a comprehensive baseline assessment within seven days, we were able to illustrate the correlation between technical and governance controls. Additionally, we were then able to route a roadmap to satisfy the regulation requirements for the next step of Building Blocks.

This established better cyber hygiene in a cost effective and efficient manner with cost justification in the strategic cybersecurity management plan.

Are You Ready to Transform Your Cyber Hygiene Controls?

Contact us at info@netswitch.net

Netswitch™
Technology Management