OPERATIONAL CHALLENGES, A COUNTRY CASE PERSPECTIVE ON KEY TRENDS, CYBERSECURITY EVOLVING THREATS, SKILLS GAPS AND NEED FOR TRANSPARENCY AND COLLABORATION.

PRESENTED BY:

LAUILEFUE AH VUI

TOPICS OF DISCUSSION

Key Trends

Evolving Cybersecurity Threats

Challenges

Our Approach

Recommendations

KEY TRENDS

5G Deployment and Innovative Applications

- 5G is revolutionizing connectivity with high-speed, low-latency networks.
- Pacific countries are adopting 5G to enable smart cities, IoT, telemedicine, and remote education.

Digital Transformation and Emerging Technologies

- Cloud computing, AI, edge computing, and network virtualization (NFV, SDN) are reshaping the telecom ecosystem, making networks smarter, faster, and more adaptable to dynamic demands.

Fiber Optic and Submarine Cable Expansion

- The Pacific relies heavily on undersea cables for international connectivity. Major investments in submarine cables are boosting global bandwidth, while FTTH (Fiber-to-the-Home) deployments are improving last-mile connectivity in urban and suburban regions.

Rural and Remote Connectivity Solutions

- Bridging the digital divide is a critical focus for governments and operators. Satellite internet (e.g., Starlink) and other innovations are bringing connectivity to underserved areas.

EVOLVING CYBERSECURITY THREATS

State Sponsored Cyber Attacks

Nature of Threat:
- Telecom companies are prime targets for state-sponsored actors aiming to intercept communications, disrupt services, or gather intelligence.

Recent Trends:
- Espionage through compromised submarine cables.
- Exploitation of telecom networks for nation-state surveillance.

Examples:
- Attacks targeting undersea cable infrastructure to eavesdrop on sensitive communications.
- Zero-day vulnerabilities exploited in telecom equipment supplied by global manufacturers.

Implication:
- Compromised critical infrastructure could disrupt regional economies and national security.

Ransomware and DDoS Attacks

Nature of Threat:
- Cybercriminal groups are increasingly targeting telecom companies with ransomware to extort money or launch DDoS attacks to disrupt services.

Recent Trends:
- Ransomware campaigns targeting critical telecom operations.
- Botnet-driven DDoS attacks leveraging IoT devices.

Examples:
- Telecom companies forced to pay ransoms to regain control of their networks.
- Large-scale outages caused by DDoS campaigns targeting backbone internet services.

Implication:
- Service disruptions can erode customer trust and result in significant financial and reputational losses.

CHALLENGES

Limited Availability of Skilled Professionals

- The region often lacks a pool of professionals trained in advanced telecom and IT skills, particularly in fields like network engineering, cybersecurity, and cloud computing.

Impact

- Reliance on foreign expertise, which can be costly and lead to delays in addressing technical challenges.
- Difficulty in maintaining and upgrading networks to meet global standards.

Retention of Skilled Workers

- Talented professionals often migrate to larger markets offering higher pay and better career opportunities.

Impact

- High turnover rates disrupt continuity and institutional knowledge

CHALLENGES

Slow adoption of Emerging Technologies

- Skill gaps slow the adoption of Technologies like 5G, IoT, and AI, which are critical for modern telecom operations

Impact

- Delays in deploying advanced services that can boost economic growth and connectivity.
- Reduced competitiveness with telecom providers in more developed regions

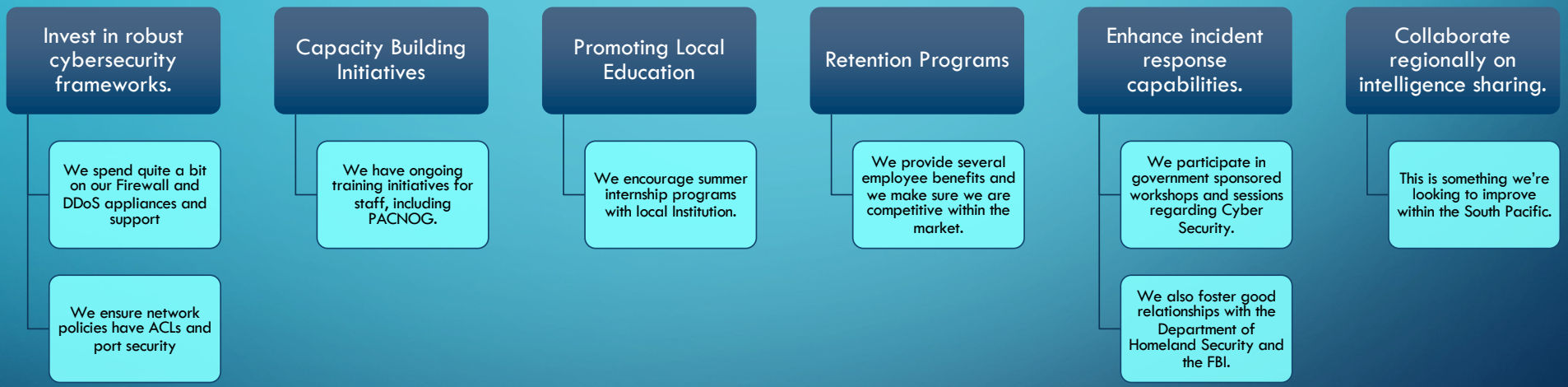
Lack of Transparency

- Organizations are wary of sharing information due to various reasons

Impact

- Hard to determine how prevalent an attack is
- Slow response to threats

OUR APPROACH



RECOMMENDATIONS

Strengthened Infrastructure Development

- Open communications about funding needs, timelines and capabilities ensures stakeholders understand priorities.
- Joint investment and maintenance of shared infrastructure, reduce costs and improve service reliability.

Ensuring Regulatory Compliance

- Helps in maintaining integrity and avoid penalties or restrictions
- Enables cooperative approaches to data protection, privacy, and consumer rights.

SUMMARY

Need for Transparency and Collaboration

- Enable telecom companies in the Pacific to overcome resource limitations.
- Build resilience against threats.
- Foster trust with stakeholders.
- Vital for promoting connectivity, economic development, and digital inclusion across the pacific region.

ANY QUESTIONS?