DAY 4 Thursday, 31 March 2022: Key Areas of E-commerce regulation and the rules proposed therein - Cybersecurity

Introduction

Cybersecurity by the numbers

TEDx: “The 5 Laws of Cybersecurity” and “Cyber Crime Isn't About Computers: It's About Behavior”

Cybersecurity – Individual level

Cyber Criminal Strategies: Social Engineering, Malware, Ransomware

Digital Attacks: Phishing, Spear Phishing, URL links, WiFi, Social Media over-sharing, Fake profiles, Trogans

Cybersecurity – Organizational level

2021 Papua New Guinea Ransomware Incident

Key questions for Executives, Board members & Government department heads

Information Security

Operational Security & Tools

Cybersecurity – National level

National CERTS and Regional Initiatives

PRIF Pacific Country Assessments (2019) & Recommendations

eCommerce Legislation

Resources

Tools, Publications, Training Programs, Courses, Workshops Links

Requests for Information

Cybersecurity (JSI-based)

The provisions of the relevant section of the JSI consolidated text are sufficiently detailed. In addressing the issues of capacity building, the text suggests taking into account the evolving nature of cybersecurity threats. As far as collaboration is concerned, the emphasis is made on anticipation, identification and mitigation of malicious intrusions and dissemination of malicious codes and using the joint mechanisms to swiftly address cybersecurity incidents, sharing information and best practices.

One of the proposals explicitly emphasizes negative influence of cybersecurity on personal data.

More substantively, risk-based (rather than prescriptive) approach is emphasized, and its benefits (such are better avoidance of trade-restrictive outcomes, accounting for evolving nature of cyber security threats) are praised. It is also suggested to ground the risk-based approach on open and transparent industry / consensus – based standards.

Finally, internet sovereignty is also acknowledged.