

# AUSTRALIA CYBER SECURITY STRATEGY 2030

Kingshuk Sinha

Cyber Security Architect



# OUR UNDERSTANDING OF CURRENT CHALLENGES IN CYBER WORLD

## Protecting Data

Loss of Customer Sensitive Data  
Loss of Organizations Sensitive  
Confidential Data

## Protecting People

Loss of personal information  
Risk of losing

## Protecting Business

Loss of customer's trust and  
Business  
Closure of Business due Cyber  
Attack

## Protecting Environment

Millennials account for about a  
quarter of the \$48 billion spent  
on other products in 2018

# Q1.IDEAS FOR SECURE NATION 2030

## Industry Based Guideline

- Australia's Cyber Security standard/guidelines should be defined based on industry ( Retail, Health,Finance etc.) using the various standards like NIST, ISM, ASD E8/E37
- Mandate use of the Australia Standard/Guidelines

## Uniform Pattern

- Standard pattern of architecture for different industry
- Approved Standard Technology /Tools for the Standard Architecture Patterns
- Predefined Configurations for the Standard tools to avoid misconfigurations and exemptions

## Awareness Campaign

- Use similar pattern to election campaign build the Digital Safety campaign or Cyber Safety Campaign
- Maximize reach among the users about Cyber Safety

## Build the Brains

- Develop Cyber Security from Primary School from year 4 onwards
- Transform malicious brain to be ethical and combat sophisticated hackers

## Q9. NOTIFICATION OF CYBER SECURITY INCIDENTS

### Communication

- Public should be well notified with Cyber Incidents
- All Industries should be notified with details of the Cyber Incident as soon as identified/detected

### Repetition

- Playbooks to tackle all the cyber incidents happened in last 2 or 3 years
- Lesson learnt from Incidents should be used to repeat in Sandbox environment

### Post-Mortem

- Root Cause for the Cyber Incidents should be provided to all the various industries

### Simplify

- Enterprise to define simplified approach to notify and openly accept if impacted by Cyber Incident
- Articulate Simple Cyber notification process across Australia



## Q12. SUPPORT AUSTRALIA'S CYBER SECURITY WORKFORCE

**Start Early**

Primary School across public and private should start teaching regularly of Cyber Safety

**Mid-Year**

Mandate Cyber Safety for High School Students from Year 7 onwards

**Transform**

Utilize Cyber Criminals and transform them and utilize brains in Ethical way

**Migrate**

Separate Cyber Security Roles defined in the skill list for migrants  
Pathway to PR for Skilled Cyber Security Professionals with specialized certifications



## Q16 OPPORTUNITIES ARE AVAILABLE FOR GOVERNMENT TO ENHANCE AUSTRALIA'S CYBER SECURITY TECHNOLOGIES ECOSYSTEM AND SUPPORT THE UPTAKE OF CYBER SECURITY SERVICES AND TECHNOLOGIES IN AUSTRALIA

- Standardize Tools across industries will reduce attack surface
- Reduce Risk of Supply chain based Cyber Attacks
- Reduce burden for industry to focus on many tools
- Industry to focus on improving feature of the standard tools
- Support and Management of Standard tools would be easy for Enterprises

# THANK YOU

Kingshuk Sinha