Future of Security

Future proofing tomorrows always on, always connected, world

Presented by
Ashutosh Kapsé,
CISM, IRAP, CRISC, ISO27001LA, CCSK, CISA, CGEIT
Head – Cybersecurity & technology risk

Disclaimer

Any logos, trademarks used, belong to the respective organisations and they own the sole right to use and reproduce them.

This presentation is intended to provide general information only and has been prepared without taking into account, any particular person's / organisation's objectives, business situation, needs or risk profile. Any person / organisation, before acting on this information, should consider the appropriateness of this information with regards to their personal / organisation's objectives, business situation, needs or risk profile. We recommend you obtain Audit and Risk advice specific to your situation before making any Risk / Audit related decisions.

Reference to any tools, technologies or organisations is not meant as endorsement, advertising or support of those products/technologies. The reference is purely to relay experiences and personal opinion.

Key points & Agenda

- Chatham house rules apply
- Show and tell
- Questions welcome anytime

1. **Cyber threats v/s Incidents**
2. **What we did - A change of focus**
3. **Key learnings**

Threats and hype

Threat horizon 2017/18 - 19

1.Rogue governments use terrorist groups to launch cyberattacks

2.Systemic vulnerabilities are weaponised

3.Dependence on CI becomes dangerous

4.Supercharged connectivity overwhelms defences

5.Crime syndicates take a quantum leap

6.Legacy technology crumbles

7.Impact of data breaches increases dramatically

8.Regulations fragment the cloud

9.Criminal capabilities expand gaps in international policing

1. Pre-meditated internet outages brings trade to its knees
2. Ransomware hijacks the Internet of Things
3. Privileged insiders coerced into giving up the crown jewels
4. Automated misinformation gains instant credibility
5. Falsified information compromises performance
6. Headlong rush to deploy AI leads to unexpected outcomes
7. Subverted blockchains shatter trust

**Source: Information Security Forum www.securityforum.org*

Incidents – common theme ?

MOSSACK FONSECA

UBER

Building a cyber security culture

What is cyber-security culture?

System of values and behaviors present in an organisation that shapes cyber risk decisions of employees and management.

Combination of

- Beliefs and Attitudes
- Principles for guiding behavior and decisions
- Management systems & processes that prioritise security
- Behaviors that foster & improve cyber security

Implement cyber-risk-aware culture

1. Accountability is important
2. “Bake-in security”
3. Educate & Reward / WIIFM
4. Leadership

Security team principles

1. Trust is our key objective
2. Foster enduring internal relationships
3. Ensure security effort is commensurate with risk (no knee jerk reactions)
4. Make secure solution easier than the existing non-secure process/solution

Educate and Reward

1. Education & learning as cornerstone.
2. Awareness / training customised for job role
3. Face to face, innovative user training
4. Don’t measure “clicks” – measure reports
5. SPoC awards
6. Educate with WIIFM as a basis

Bake-in security

1. Security champions
2. Avoid compliance / checkbox mentality
3. Avoid us/them - “dotted line” reporting
4. Security presence in key areas – CAB, threat modelling, procurement, legal etc.

Leadership

Cybersecurity leadership touches all parts of the business

The Board

Security leadership is providing guidance for governance, committing appropriate resources.

The CEO

-Being a role model that sets risk tolerance culture

-Through action communicates what due care looks like (tone from top)

The CISO

-Foster enduring internal relationships

-Focus on enabling business securely

-Ensure technology team is undertaking technology hygiene as BAU

Key learning

With appropriate focus on

- “Cyber risk aware culture” development,
- Leadership from security
- Using “Trust” as key objective

organisations can bring about fundamental and lasting improvement to the cyber security posture.

- Cultural change is hard
- Behaviours can be measured / culture cannot be
- This is a long process taking years

Questions ?

Contacts:

Ashutosh Kapsé
ashutosh.kapse@ioof.com.au
0418990305
Twitter: iAshutoshKapse