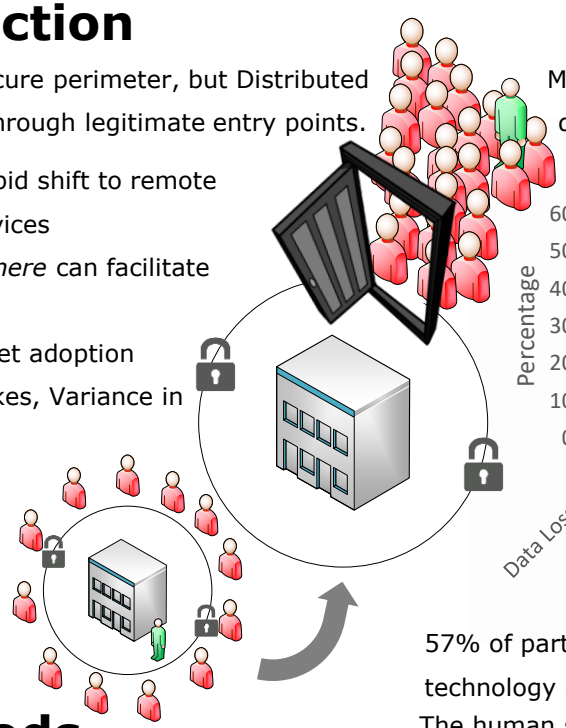
DDoS Readiness and Capability

Mr. Ian Wiltshire, A/Professor Sujana Adapa, Dr David Paul
Faculty of Science, Agriculture, Business and Law - University of New England

Introduction

Traditional cyber defence uses a secure perimeter, but Distributed Denial of Service (DDoS) disrupts through legitimate entry points.

- Threat landscape enlarged by rapid shift to remote working and explosion of IoT devices
- Cloud technologies *Access Anywhere* can facilitate Attack from Anywhere
- DDoS growing faster than Internet adoption
- Human factor a weak link. Mistakes, Variance in approach, Cultural difference



Methods

This project followed an exploratory research methodology to uncover macro and micro themes relating to the perception of DDoS in SMEs.

Website analysis of 48 Websites

30 Semi Structured Interviews, via videoconference

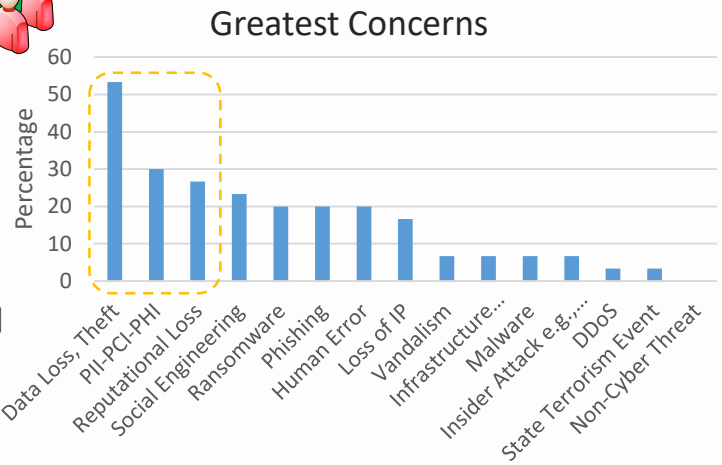
Initial exploration of macro themes in Microsoft Excel

Micro themes qualitative analysis in NVivo

Australian Computer Science Week 2022

Results

Most participants believe DDoS is a credible threat, but data loss and reputational damage is more concerning

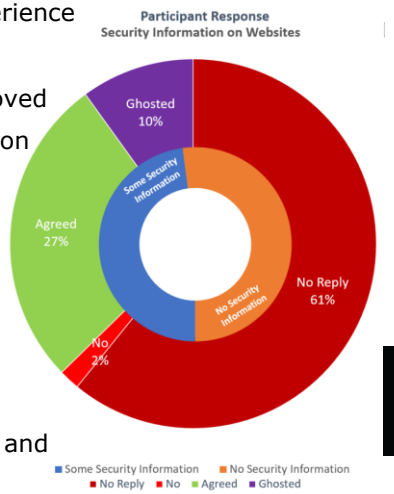


57% of participants had a plan for DDoS but these plans focus on technology and process

The human side may be neglected as:

- employees request more peer experience be shared and,
- their skills and knowledge be improved
- websites without security information use simpler language (Flesch–Kincaid)

- Sharing cyber security information and experience is rare



Implications

The adoption of DDoS by criminals, the explosive growth of IoT and the rapid adoption of remote working has increased the threat to ALL organisations

- Infrequent training and the lack of shared experiences may mean employees are ill-prepared for an attack, even if they have capable technology and process
- Networked products which lack any form of cyber security standard mean insecure devices configured by untrained home owners could be ready for use by DDoS attackers

Conclusion

- Threat is growing and now an attack tool used by criminals
- Home working has increased the threat landscape.
  - E.g. Poor quality insecure equipment, IoT, Home owners performing shadow IT
- Human factor is a major risk – Employees must carry the organisations security posture to the home even when not monitored
- Training and Sharing are the way forward

Acknowledgements

Special thanks to my supervisors, A/Professor Sujana Adapa & Dr David Paul and the UNE Faculty of Science, Agriculture, Business and Law

Ian Wiltshire
iwiltshi@myune.edu.au