

Cyber Threats and Incident Response

Tom Fairfax

Head of Advisory Services

SRM Ltd

Managing your Known Unknowns

Apologies to DR

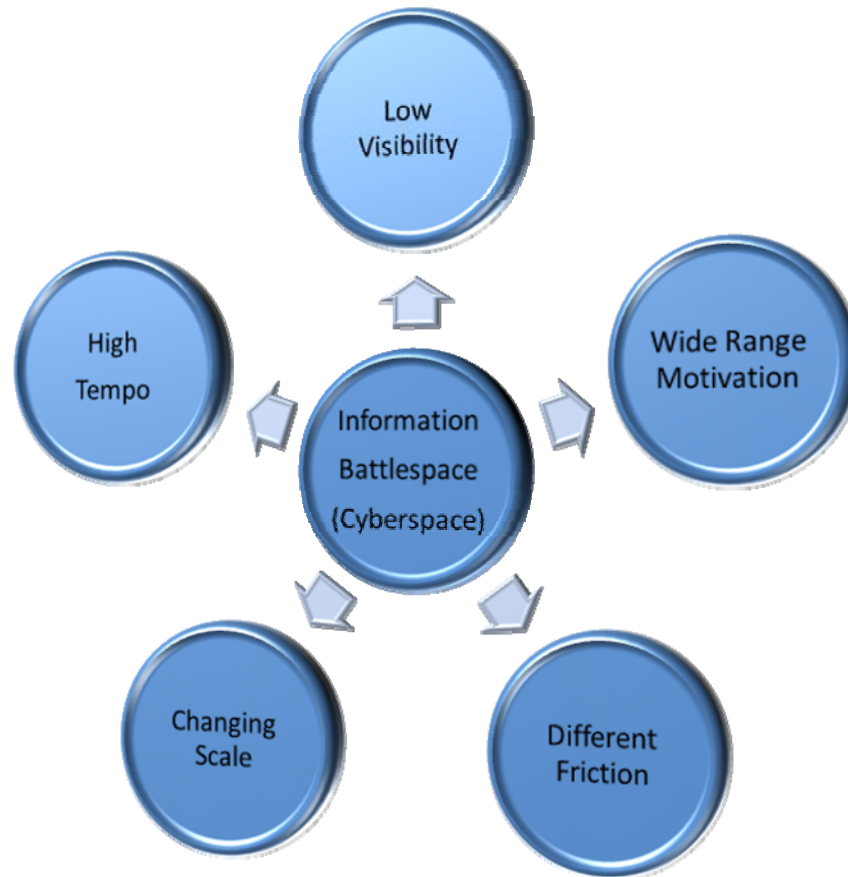
Core Objectives

- Presentation
 - Discuss an approach to managing threat in cyberspace.
- Key Management Objectives
 - Understand what is happening
 - Seize Initiative
 - Manage Situation

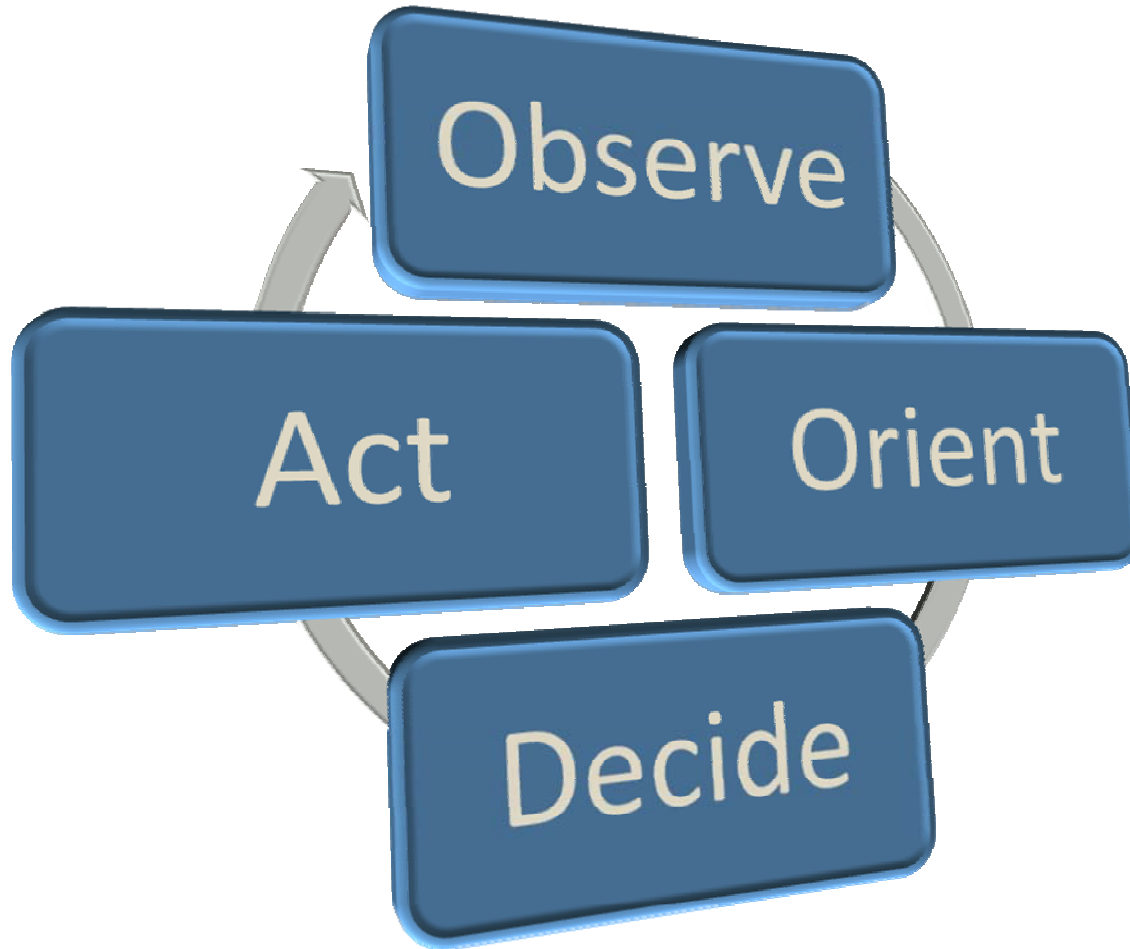
Approach

- Chatham House Rule
- Key Concepts
 - Characteristics of Cyberspace
 - Decision Making
- Understanding the system
 - MITB – A complex example
 - Data Compromise – a typical example

Characteristics of Cyberspace



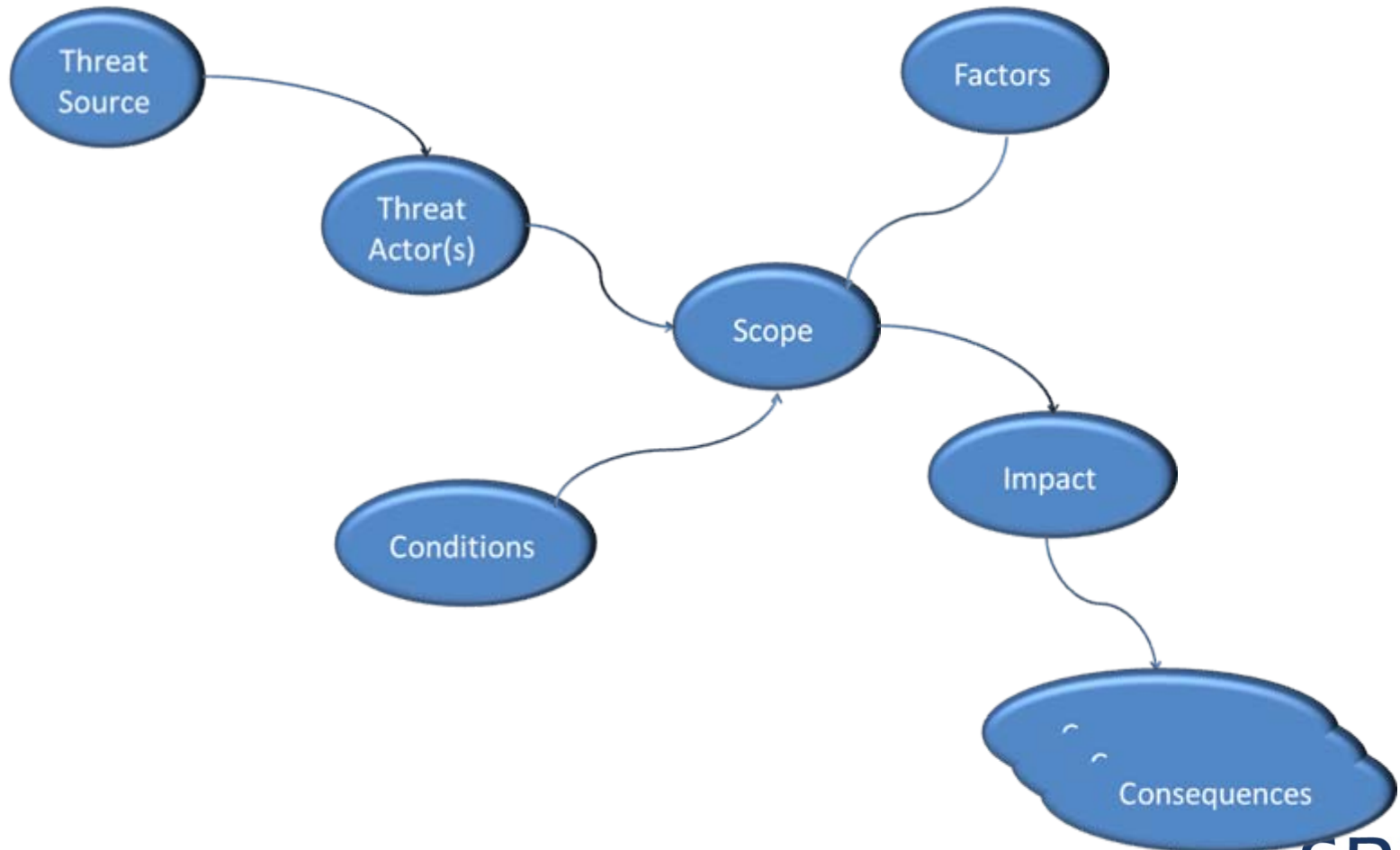
Decision Cycle – The “OODA” Loop



SRM

Consultancy. Outsourcing. Technology.

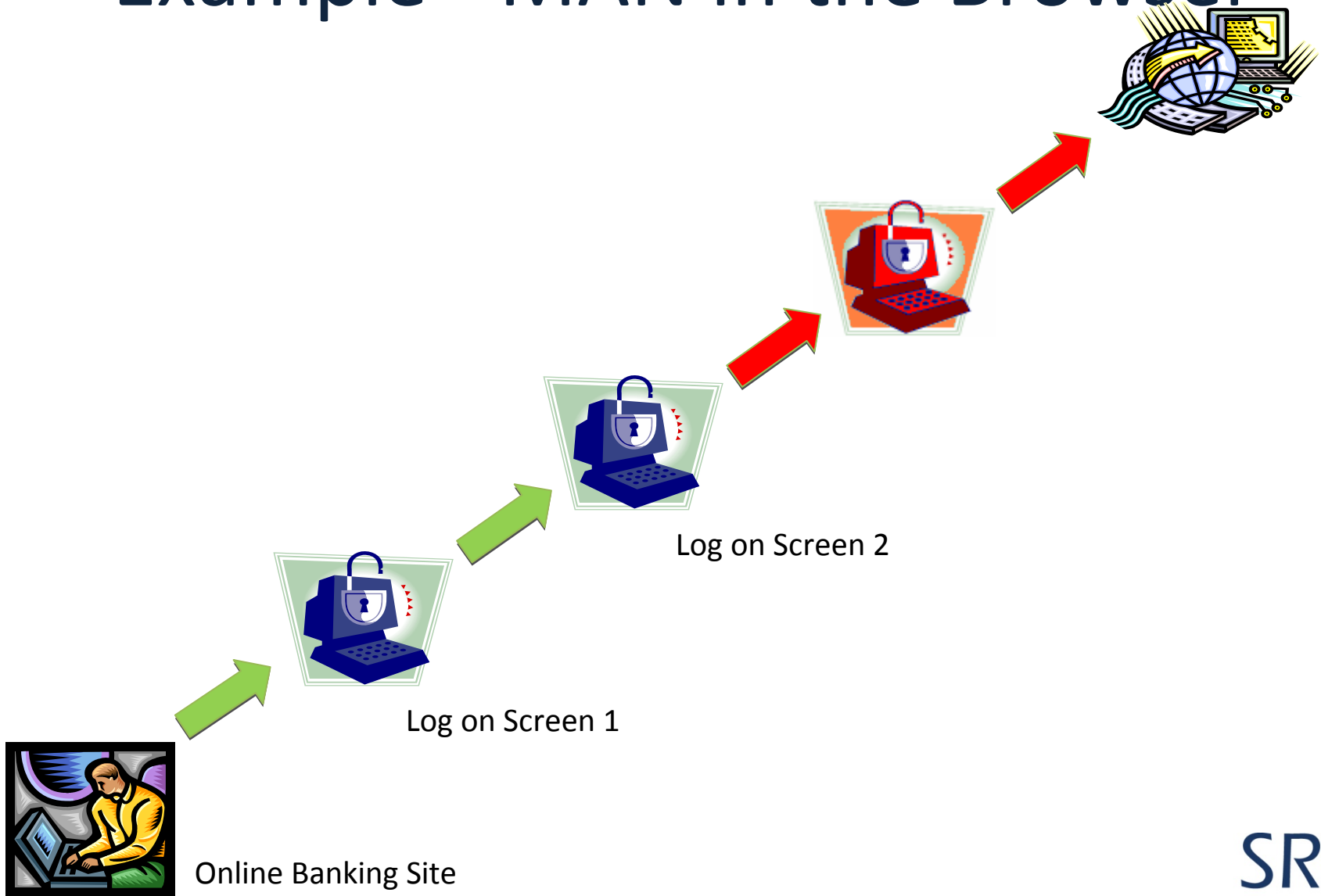
Understand what's involved!



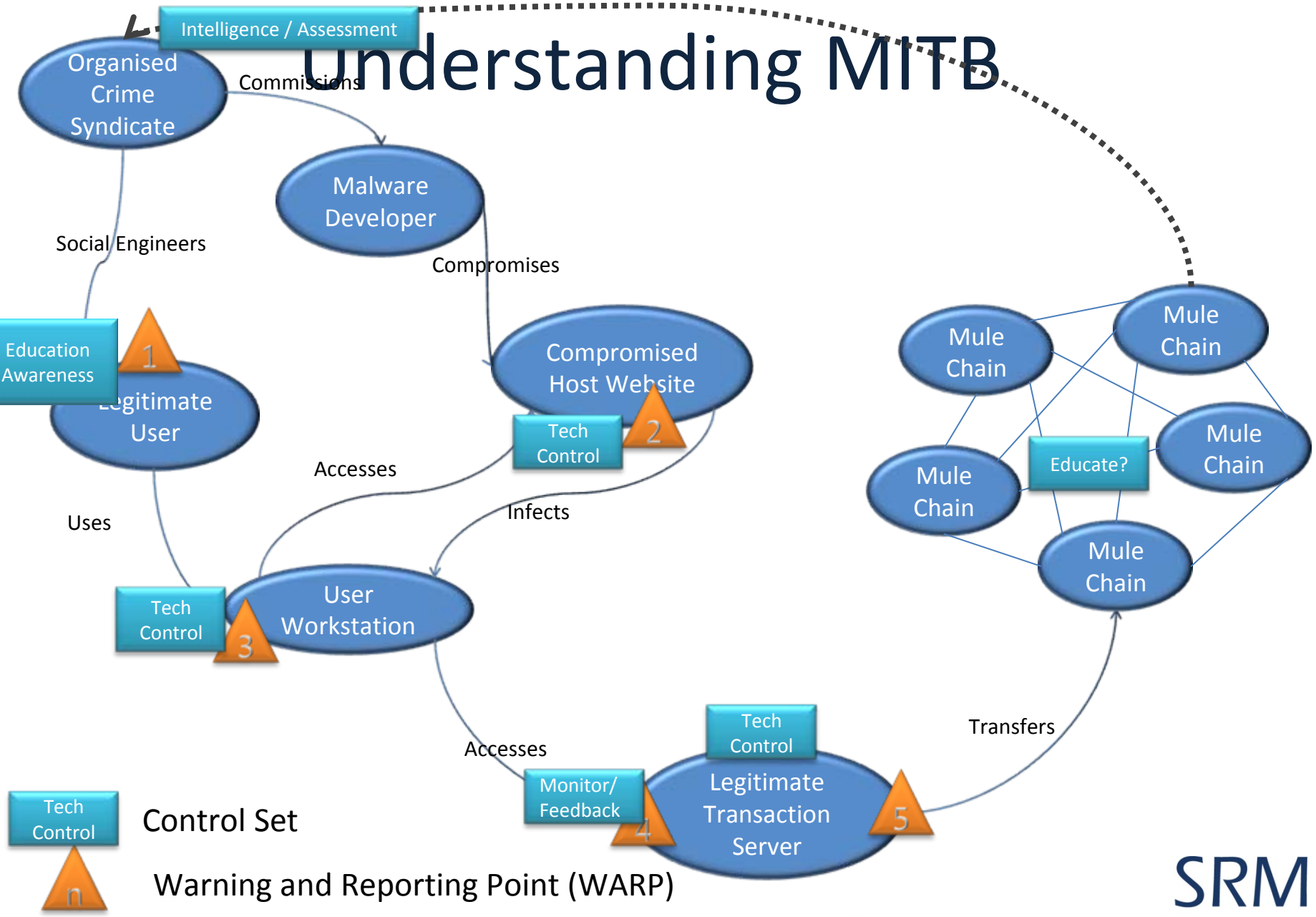
SRM

Consultancy. Outsourcing. Technology.

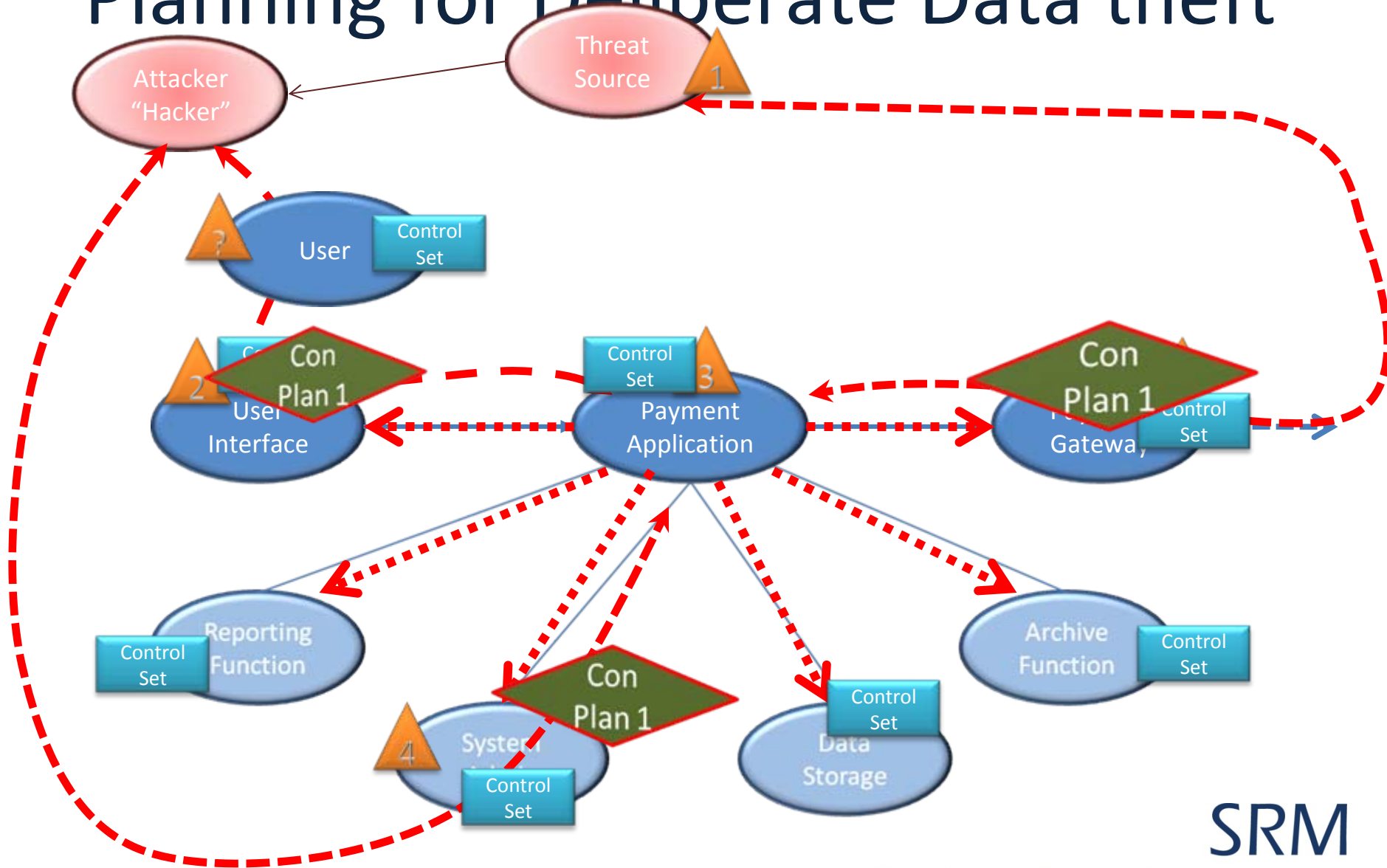
Example - MAN in the Browser



Understanding MITB



Planning for Deliberate Data theft



Summary

- Understand the environment
 - Make it Visible
 - Make it Tangible
 - Keep it Simple
- Know the unknowns.....