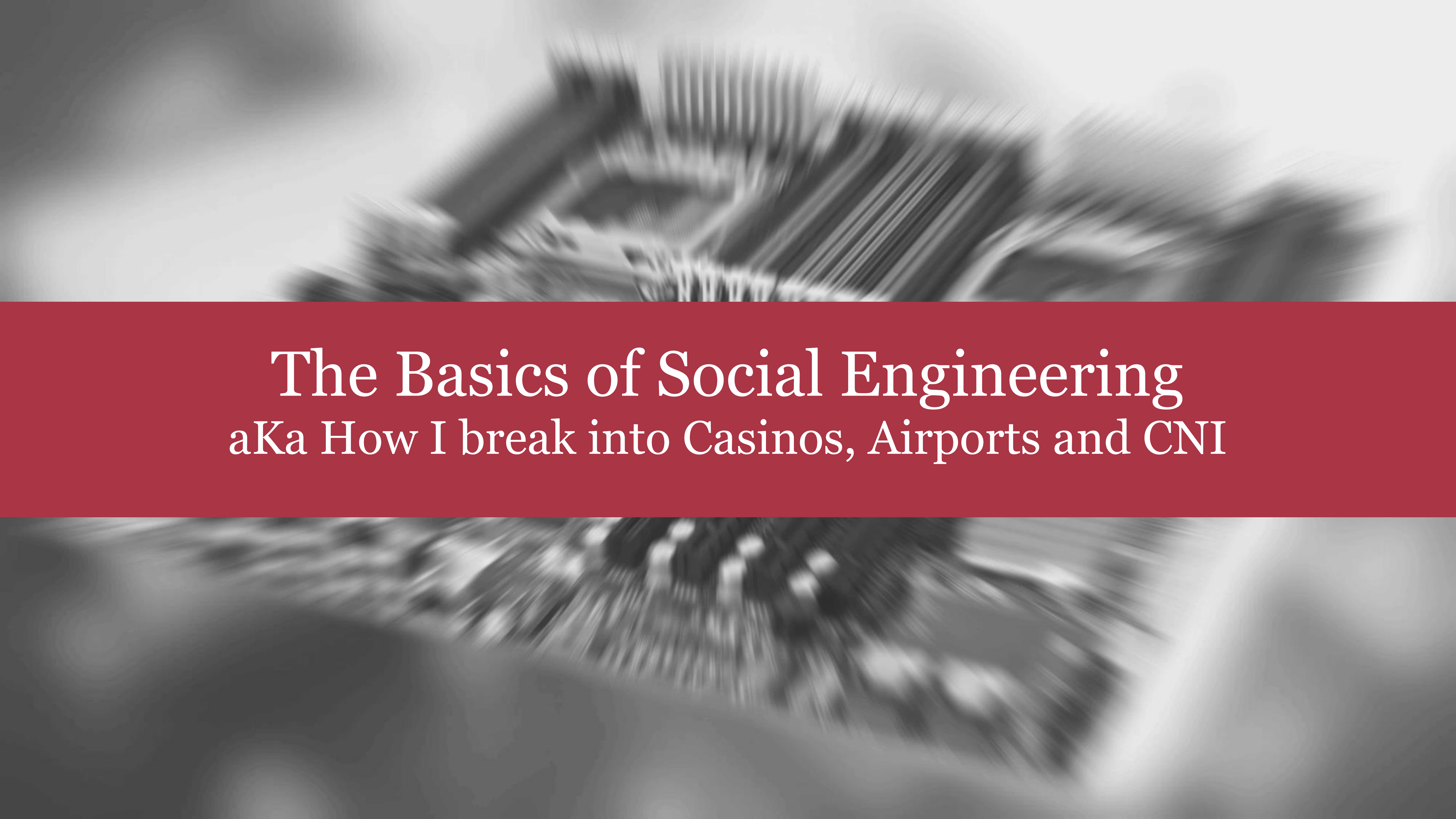

The Basics of Social Engineering

aKa How I break into Casinos, Airports and CNI

Terminology

- SE – Social Engineering
- CNI – Critical National Infrastructure
- OSINT – Open Source Intelligence
- Pretext - A reason given in justification of a course of action that is not the real reason
- NDA – No Comment

Step 1 - Reconnaissance

- Perform OSINT on the target, Google Maps, Street View, their web site
- Walk the building/perimeter
    - Back Entrances?
    - Smoking Shed?
    - Shared Office?
    - Sit in reception
- What are staff wearing? Office wear? Smart casual? Something else?
- What else do you notice? ID Badges? How do they wear them? Lanyards? Metal Pin Badges on the lanyard?
- When are the busy entry/exit times? When are the quiet times?

Step 2 – After Recon, Before Entry

- Construct your pretext
    - Fit it around your knowledge
    - Shroud a story in part truth and it becomes believable
- Get your outfit on, match their dress style (pretext dependant)
- Remember your props (Pretext = IT Network? Bring a laptop, and CAT5 cable)
- Get there on time (The time you want to enter)

Step 3 – You're in! Now What?!

- Keep Calm!!
- You saw maps & pics from the OSINT, now relate those to where you are
- Be observant
  - Where are the toilets?! (hide in them and relax, let the adrenaline subside)
  - Where are the exits?
  - Are they push button exits, or swipe card controlled?

Step 3 – You’re in! Now What?! – Cont’d

- What’s the target?
- Don’t be afraid to ask for help
- Engage in “colleague” related chit chat (you work there remember)
- Always leave people feeling better for having met you
  - It’s useful to return to your new “friend”
  - Builds acceptance that you should be there
- Just one piece of psychology related advice…..
  - Don’t negate the frame (Don’t think about pink elephants!)

You’ve Done It – What Else Do You Need?

The Fear

Nerves are natural

Hide in that toilet

It’s exhausting

No really, it is exhausting!

How to get over those ethics? Tell yourself that you’re just acting

Next Steps?

- Read books, here’s some suggestions:
  - Amy Cuddy – Presence
  - Olivia Fox Cabane – The Charisma Myth
  - Ian Mann – Hacking the human
  - Chris Hadnagy – The Art of Social Engineering
- Practice, Practice, Practice!

The End

Thank you!

Questions?

(feedback welcome, @ghostie_)

✉ info@pentestpartners.com

☎ +44 (0)20 3095 0500

@PenTestPartners

PenTestPartnersLLP