

# The fundamental drivers of human behaviour in cyber security





# Contents

- 1. Thinking beyond the tech
- 2. Human behaviour and cyber security
- 3. What should we do about it?

# Thinking beyond the tech

- Cyber security is a big ecosystem
- Divide between tech vs non-tech people distorts and damages cyber security
- Focus on people, not technology

# Health model

## Variety of roles

- specialists
- generalists
- allied health

## Variety of activities

- monitoring
- incident response
- epidemiology
- immunisation
- education

# Human behaviour

- Well-recognised, but under-examined
- More than just behavioural analytics
- We need to work **with**, not **against**

# Humanity and computing

- We've had 70 years of getting people to work on computers' terms
- But, for cyber security to work, we need computers to work on our terms



# Human brain

- analogue
- awful memory
- terrible at algorithms and calculation
- great pattern recognition
- awesomely adaptable

# Dirty dozen

- Lack of communication
- Lack of resources
- Lack of knowledge
- Lack of assertiveness
- Lack of teamwork
- Lack of awareness
- Distraction
- Stress
- Complacency
- Pressure
- Fatigue
- Norms

# Five factors

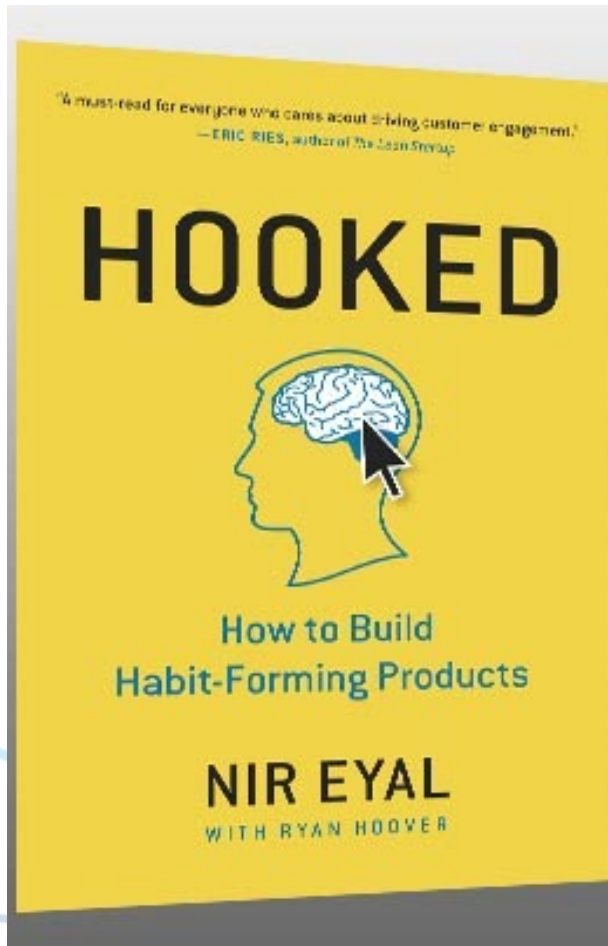
- lack of knowledge
- poor role models
- takes too long
- sceptical attitude
- the technology is inconvenient
- (2002 US Hand Hygiene Task Force)

# Habit forming

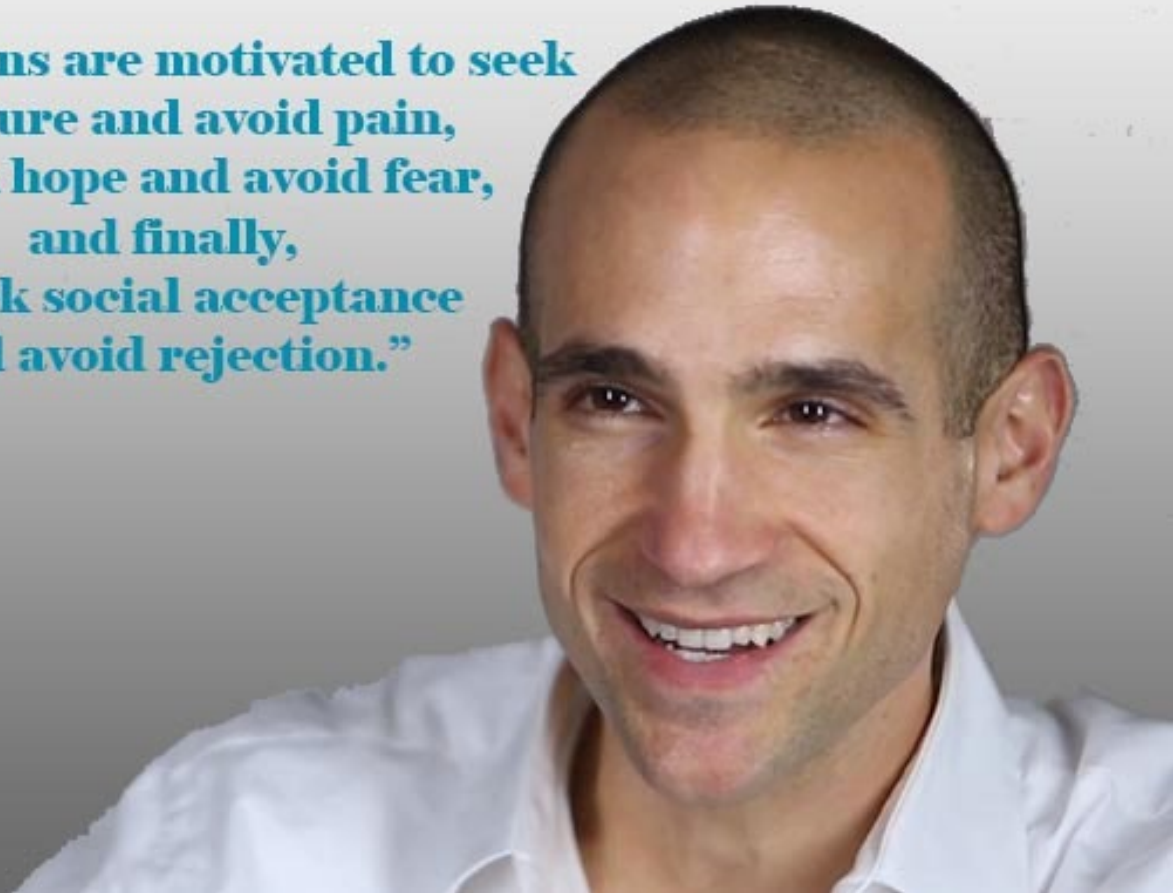
- Gambling industry built on exploiting human weakness
- App designers have integrated the lessons from the gambling industry



# Habit forming



**“All humans are motivated to seek pleasure and avoid pain, to seek hope and avoid fear, and finally, to seek social acceptance and avoid rejection.”**



# Hook loop

- 1 a) **External trigger:** mechanisms telling you to act
- 1 b) **Internal trigger:**
  - Seeking pleasure / Avoiding pain
  - Seeking hope / Avoiding fear
  - Seeking acceptance / Avoiding rejection
- 2) **Action:** easy, fast, inexpensive
- 3) **Reward:** randomised but at least sufficient
- 4) **Investment:** time, money

# So what should we do?

- Three actions that are complementary:
  - 1. Humanise cyber
  - 2. Positivise cyber into 'cyber wellness'
  - 3. Become storytellers

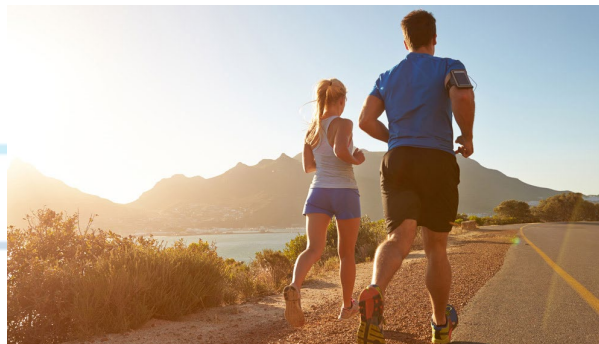


# 1. Humanise cyber

- Think beyond the tech
- Cyber security ecosystem
- Human behaviour is not going to change
- Make computers work on human terms, not the other way around!
- Practice more empathy
- Start with 'why'

# 2. Positivise cyber

- Flip the normal narrative
- Cyber is a bit like counter terrorism – success is nothing happening
- Health metaphor again, we need 'cyber wellness'



# 3. Be a storyteller

- “Biggest problem in communication is the illusion that it has taken place”
- Claremont Graduate University research on oxytocin

# What's AustCyber doing?



- Sector Competitiveness Plan – [scp.acsgn.com](http://scp.acsgn.com)
- 3 goals:
  - Grow the ecosystem
  - Export our capability
  - Become a leading centre for education
- We exist because cyber is Australia's 100 year opportunity

# Knowledge priorities

- 1. Emerging prevention, detection and response technologies
- 2. Identity, authentication and authorisation in the cyber domain
- 3. Ensuring security, privacy, trust and ethical use of emerging technologies
- **4. Approaches to deal with the increasingly 'shared' responsibility of cyber security**
  - **Human behaviour a key part of this**

# Thanks!



## Mike Bareja

Email: [mike@austcyber.com](mailto:mike@austcyber.com)

Twitter: [@mikebex](https://twitter.com/mikebex)

LinkedIn: [mike-bareja](https://www.linkedin.com/in/mike-bareja)

## AustCyber

Web: [www.austcyber.com](http://www.austcyber.com)

Email: [info@austcyber.com](mailto:info@austcyber.com)

Twitter: [@austcyber](https://twitter.com/austcyber)

[@cyber\\_roo](https://twitter.com/cyber_roo)

Become a friend of the network: [austcyber.com/connect](http://austcyber.com/connect)