Security is a State of Mind, not a State.

David Higgins
External High Risk Programme Reviewer @ IPA
Hands up all those who.....

- Think that their organisation is secure.
- Absolutely, *definitely* know that their organisation is secure.
- Would risk the life of a child or much loved pet based on their organisations security capability.
Firstly..

Checking in with expert Bruce Schneier about the state of security.

Jon Erickson
*Dr. Dobb’s Journal*
October 1, 2008

“Where we need work is in the human aspects of security: Installation and configuration, user interface, education, even economic and psychological motivations and limitations. The biggest step forward in recent years is the increasing recognition that these issues are central to security and not marginal concerns.”

......that the commercial Cyber world is missing an opportunity in not adopting the classic skills associated with HUMINT. Skills such as cognitive thinking about human drivers behind the threat perimeter and ‘active targeting’ would increase our ability to interdict malicious activity prior to compromise and would gain useful intelligence on an opponent’s motivation, disposition and intentions.
More Recently…

Shireen Walton • 1st
Agile Coach-Cyber and Technology at Severn Trent
Gloucester, United Kingdom

An inquiry into a theoretical framework for Cyber and Positive Psychology:
Approaches and Applications.

Smart, Cyber, Security, Programme and Technology Consulting
More Recently Still...

Security is a state of mind, not a state.

Security is what you think it is, a subjective assessment, based on personal psychological frameworks, driven by, and supported by the macro environment.

https://www.linkedin.com/pulse/security-state-mind-david-higgins/
Risk Assessment as an Art Not a Science

Thinking about security risk…

- Risk Frameworks
- Threat Intelligence
- Threat perimeter perceptions
- Team and organisational dynamics
- The macro environment
- Personal psychological frameworks (aka “Risk tolerance”)
Measuring Personalities

What approaches can we use to measure the make up of overall personality structure of security risk assessment teams?

O.C.E.A.N.

• Openness
• Conscientiousness
• Extraversion
• Agreeableness
• Neuroticism

OCEAN – Personality Fundamentals

Personality

- Openness
- Neuroticism
- Conscientiousness
- Agreeableness
- Extraversion
Mapping the Ocean
Mapping the Ocean

- Openness
- Conscioussness
- Neuroticism
- Agreeableness
- Extraversion

Defender
Defender
Defender
Mapping the Ocean

Openness
Neuroticism
Agreeableness
Extraversion
Consciousness

Defender
Defender
Defender
Blended
Mapping the Ocean

![Diagram showing the relationship between Openness, Neuroticism, Conscientiousness, Agreeableness, and Extraversion with two lines: Blended and Attacker.](image-url)
Mapping the Ocean – the disposition gap
Beyond the Ocean

Other complicating factors:

- **Groupthink** – The social dynamics of a situation override the best outcomes.
- **Confirmation Bias** – Looking for ways to justify your existing beliefs.
- **Belief Bias** – If a conclusion supports your existing beliefs then you’ll rationalise anything that supports it.
- **In-Group Bias** – favouring those who belong in your group.
- **Reactance** – Doing the opposite of what someone is trying to make you do.

*World Economic Forum – 24 Cognitive biases that are warping your perception of reality*
Is there a naturally occurring Cyber Psychology ‘Sweet-Spot’?

And, if there isn’t, what can we do about it?
‘Sweet-Spot’ Analysis – In Progress

• Questionnaire based assessment of the individual and group profiles of cyber defenders – currently in progress at two CNI related sites.

• Sadly the opposition won’t currently fill out the questionnaires so any assessment of their profiles will need to be based on behavioural reverse engineering for now.

• Looking for commonality and disparity in defender profiles.
In the Meantime…

• Ensure that you have explicit psychological diversity in the risk assessment process.

• Look for, and avoid Groupthink, In-Group bias, Conformation Bias.

• Be aware of belief bias – e.g. it won’t happen to us (security through insignificance isn’t a defensive strategy).

• Psychological flexibility (aka Neuroplasticity) will help.
Neuroplasticity in Action
Are Threat Actors Also Using This Approach?

They are – as a method of creating information warfare campaigns as well as targeted “under pressure” attacks specifically designed to exploit the psychological make up of defender teams and high value asset owners.

In Summary

- Lots of work in progress.
- Government interest in the model.
- We’re seeing early signs of threat actor interest in this area.
- We need to be more aware of the impact of psychological profiles as part of the risk assessment process.
Any Questions?
Want to learn more / take part?

Contact details:

David.Higgins@one4solutions.co.uk
Security is a State of Mind, not a State.

David Higgins
External High Risk Programme Reviewer @ IPA