Cybersecurity starts with people

Ovidiu Popeti
Head of Government Affairs & Partnerships
OutThink

The $25M voicemail

watch

Jaguar Land Rover hack has cost UK economy £1.9bn, experts say

The Guardian

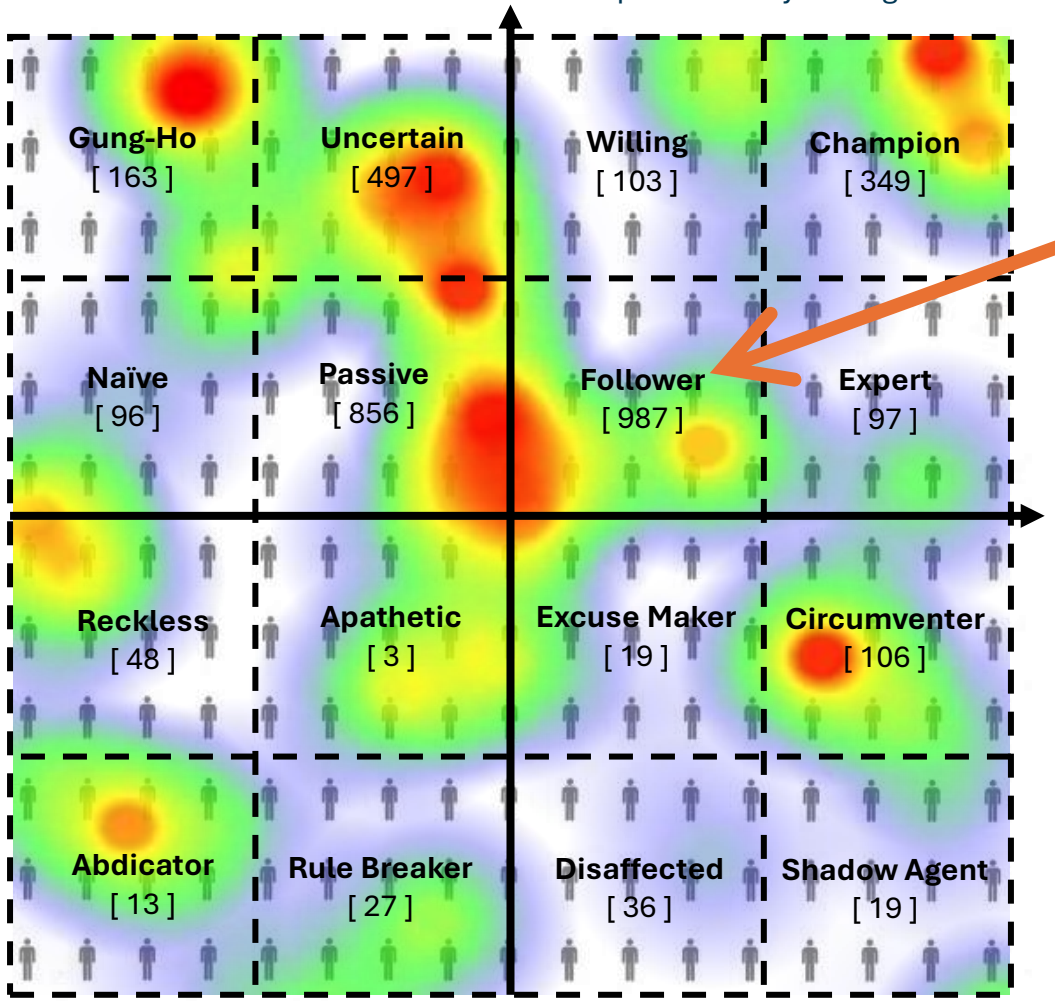
In 2024, 95% of data breaches were tied to human error, with cybersecurity protections often breaking down due to *poorly trained users*.

WEF Cybersecurity

No Two Users Are The Same

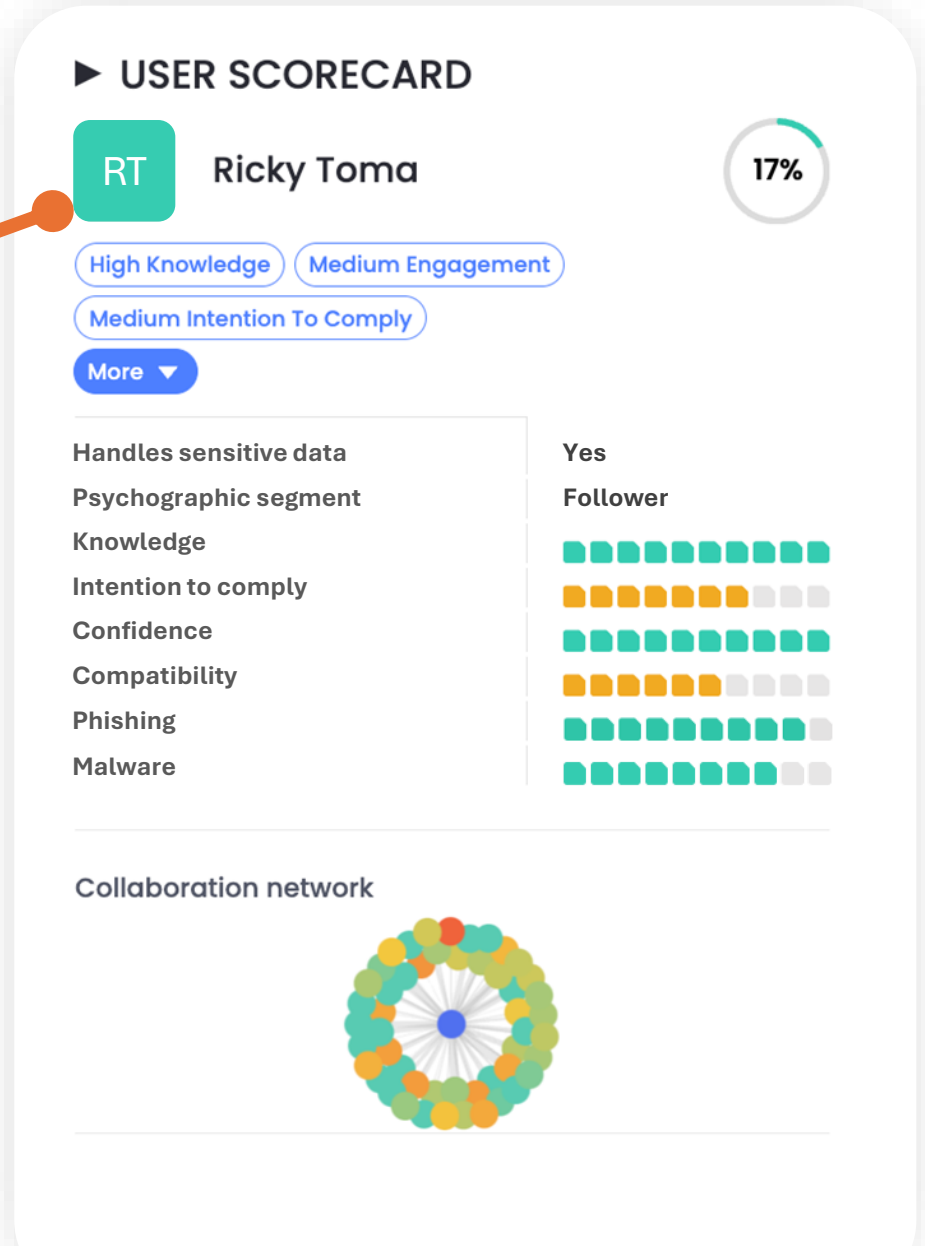
AS

***'Affective Security'* (AS)**
shows the individual's emotional response to security, as represented by the organization's security policy.



RU

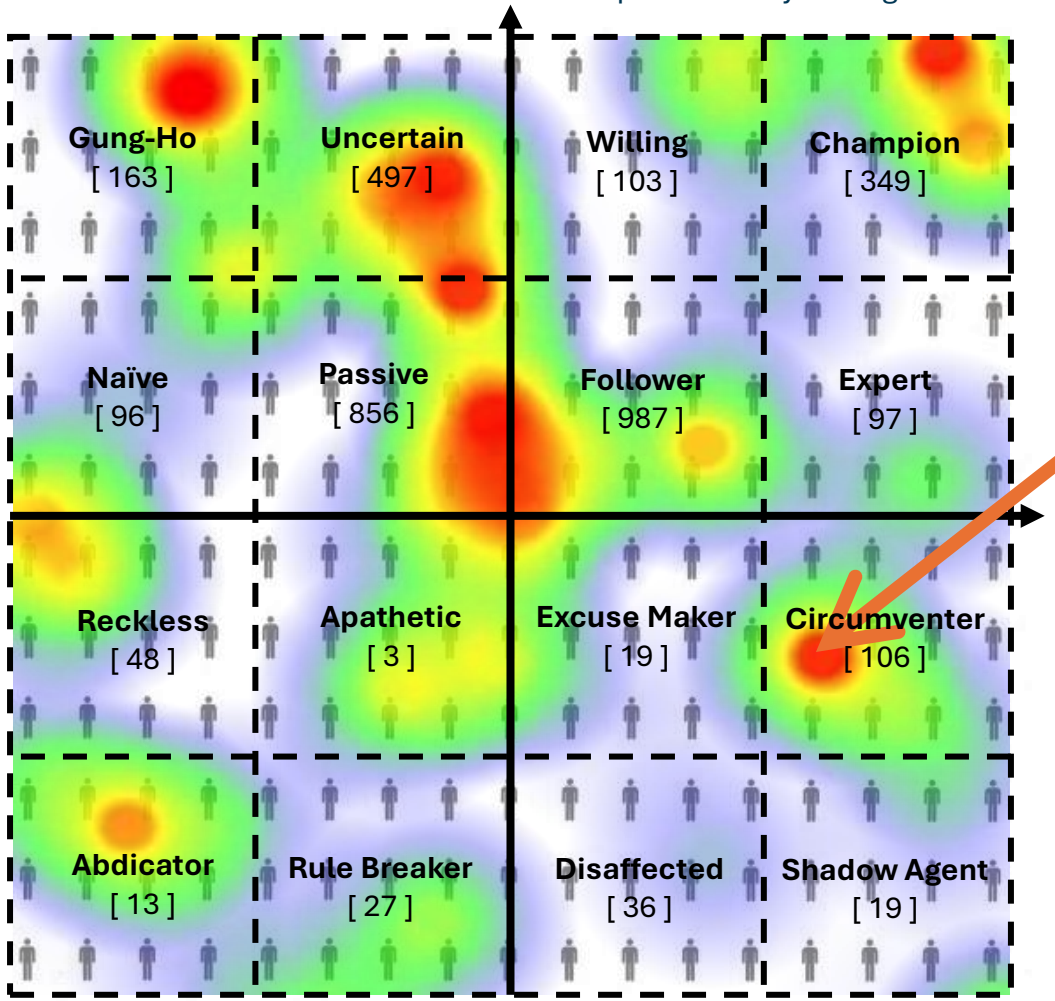
***'Risk Understanding'* (RU)**
denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.



No Two Users Are The Same

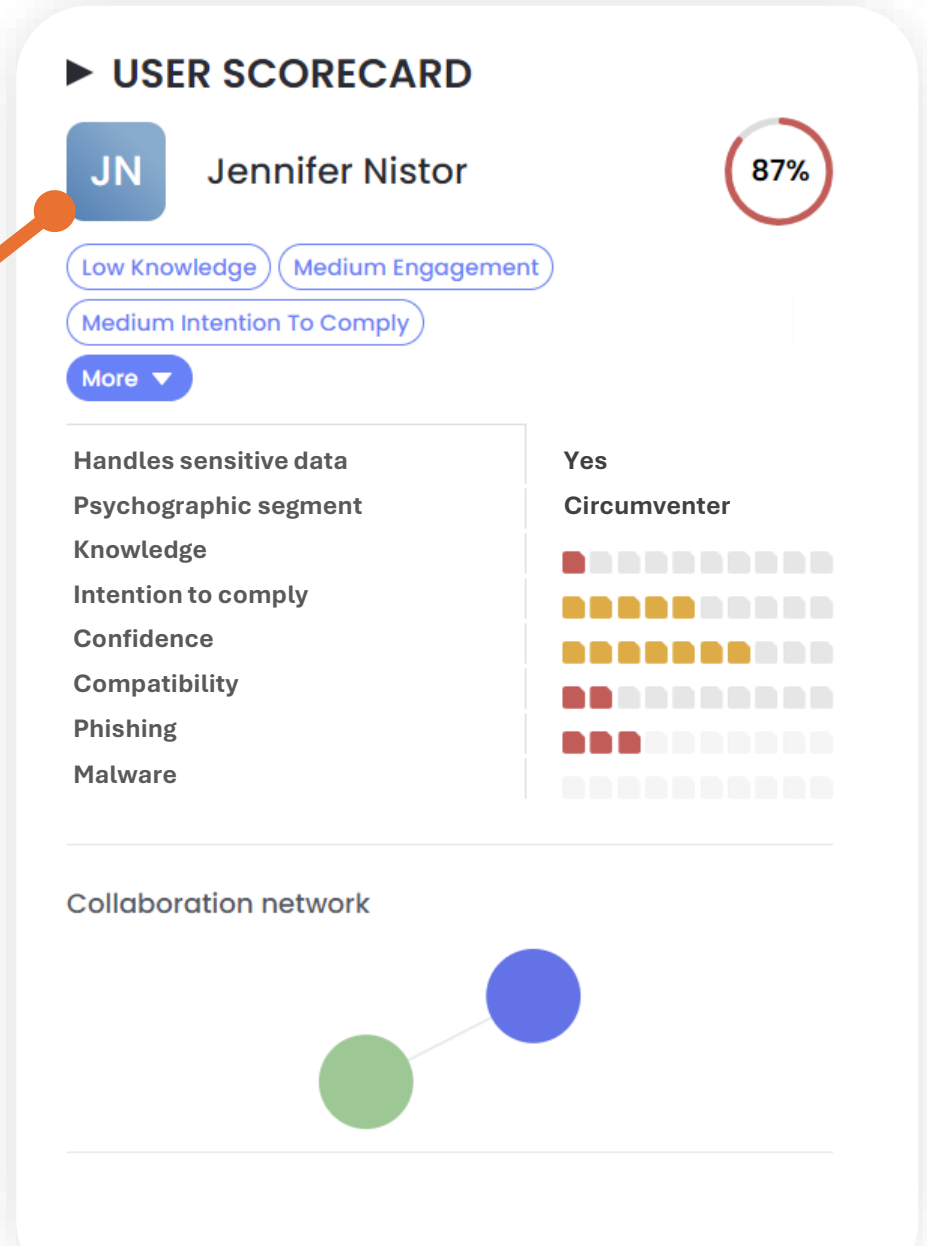
AS

***'Affective Security'* (AS)**
shows the individual's emotional response to security, as represented by the organization's security policy.



RU

***'Risk Understanding'* (RU)**
denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.



2019

OutThink was founded by 5 CISOs

2021

Secured support from the European Innovation Council

2022

Secured $10m in investment

2025

Over 10m users engaged and trained

Our vision is to secure digital life, everywhere.

M. Angela Sasse · 1st

Professor at Ruhr University Bochum, Emeritus Professor at UCL

Bochum, North Rhine-Westphalia, Germany · Contact info

Ruhr University Bochum

The University of Birmingham

About

Security research
Human Behaviour in Security
Security awareness, education & training

Chief Scientifc Advisor
OutThink
Jan 2018 - Present · 8 yrs 5 mos

Chief Scientific Advisor
iProov
Jun 2012 - Present · 14 yrs

University College London
35 yrs 7 mos

- **Professor of Human-Centred Technology**
  Oct 2003 - Present · 22 yrs 8 mos

Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors

Odette Beris
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
Tel: +44 (0)20 7679 2788
odette.beris.12@ucl.ac.uk

Adam Beautement
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
Tel: +44 (0)20 7679 0353
a.beautement@cs.ucl.ac.uk

M. Angela Sasse
University College London
Department of Computer Science
Malet Place, London, WC1E 6BT
Tel: +44 (0)20 7679 7212
a.sasse@cs.ucl.ac.uk

ABSTRACT

We introduce a new methodology for identifying the factors that drive employee security behaviors in organizations, based on a well-known paradigm from psychology, the *Johari Window*. An analysis of 93 interviews with staff from 2 multinational organizations revealed that security behavior is driven by a combination of *risk understanding* and *emotional stance* towards security policy. Furthermore, we found that a quantitative analysis of these dimensions is capable of differentiating between the staff populations of the two organizations. Organization B showed a healthier set of security behaviors, as a result of its employees having better risk understanding and a more positive emotional stance. The framework distinguishes between 16 theoretical behavioral types, (3 of which are *rule breakers*, *excuse makers* and *security champions*). It can be used to identify groups of employees that potentially pose a risk to the organization, as well as those with beneficial skills and expertise. This allows highly specific messages to be targeted to change the risk perception and emotional stance of such groups. Assuming the organization has ensured *security hygiene* (i.e. its policies can be complied with in the context of productive activity), this can shift behavior towards compliance. Our framework thus offers diagnostic and intervention-shaping tools for the next step in improving security culture.

Categories and Subject Descriptors

General Terms

Risk Perception, Emotion, Information Security,

Keywords

Risk Perception, Risk Understanding, Affect, Emotion, Information Security, Security Policy.

1. INTRODUCTION

NSPW'15, September 8-11, 2015 Twente, The Netherlands
ISBN 978-1-4503-3743-0

Employees who do not comply with security policies are a key risk for organizations trying to protect systems and data. Schneier is often quoted as saying people are *"the weakest link in the security chain"* [1]. Whilst this statement has some essence of truth, it is too often used as a justification for blaming people for being uneducated or lazy. However, this assumption does nothing to improve the situation; employees are an essential component of an organization's security posture, and their behavior is a key resource that must be effectively managed effectively, just like any other resource [2]. As Pallas [3] states *"security management is all about human behavior"*. Even when organizations recognize that successful security management involves managing undesirable security behavior, what constitutes an effective response is less clear. They typically treat their staff as a homogenous group, rather than a collection of individuals with differing security attitudes, levels of knowledge, goals and tasks. However, pushing the same messages to all staff creates information overload and additional security tasks. Where security-related work distracts users from their main productive activity friction between business and security is created. People have a limited tolerance for friction and disruption. When this tolerance, their *Compliance Budget* [4] is exceeded, they will be tempted not to comply. Most non-compliance is not lazy or malicious, but occurs because security is seen as an onerous overhead and a distraction from an employee's primary task or day-to-day role [4]. Employees may also circumvent security rules because the policy itself, and the associated technical mechanisms, are not fit for purpose in the business environment [5]. Recent research has identified a pattern of behavior referred to as 'shadow security' where employees create workarounds when 'official' security is too burdensome, yet are still security-conscious and take other measures to protect against the risks they understand. Management is often unaware that employees are operating in this fashion [6].

While compliance with policy is no guarantee of security, in many cases a failure to comply, and the associated workarounds that replace sanctioned processes, creates new vulnerabilities. We agree that compliance is desirable, but trying to enforce polices and mechanisms that are unworkable in the context to which they are deployed is futile. Organizations must perform essential *security hygiene*, a process of identifying and re-designing high-friction security [7]. Security hygiene is a necessary, but not sufficient condition for compliance: staff may still be tempted to cut corners where they perceive risks as negligible, or think the organization does not 'deserve' their contribution to security. It is this 'next layer' of influencing security behavior our paper targets.

Security managers typically only consider lack of knowledge - specifically not appreciating the severity of a risk as a driver of

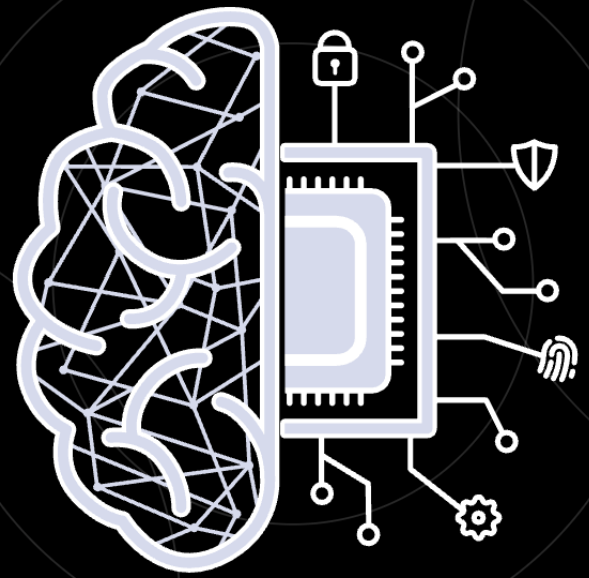
OutThink

Adaptive Training

Increase users' resilience to cyberattacks

+ Train & Engage Your People

+ Build Phishing Resilience



Adaptive Security

Prevent human-initiated security incidents

+ Build Effective & Sustainable Security

+ Automate Conditional Access & Security Controls Co-build

Human Risk Intelligence

Cybersecurity is not a technical skill, but a life skill.

Thank you!