Effective Security for the Post-compliance Era

Security Awareness and Training for Security Specialists

M. ANGELA SASSE, RUHR UNIVERSITY BOCHUM & UCL
The problem
Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity
Typical characterisation of users

“the lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of users’ mistakes”

“There was little evidence that there are specific links between types of people (e.g. gender, personality) and security behaviours.”
Self-efficacy

“self-efficacy was a reliable, moderately strong predictor of cyber-security intention and behaviour. This suggests that interventions that seek to improve users’ ability to respond appropriately to cyber-threats (and belief that those responses will be effective) is more likely to yield positive results than campaigns based around stressing the threat.”

Which is why FUD is so counter-productive …
Stop trying to fix people – fix your security

“by systematically approaching and analysing the current cybersecurity stance of the organisation, and carrying out an in-depth analysis of the causes of any problem(s), ENISA proposes that practitioners can take significant steps towards helping employees to act in a more secure way. This may involve skills-based training and support but may also require the restructuring of security practises and policies to better align with people’s workplace goals and/or capabilities.”

“We cannot change the human condition – but we can change the condition under which humans work.”

James Reason
Problem 1: Impossible security

“Never give an order that can’t be obeyed”
General Douglas MacArthur 1880-1964
The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1-d!

Bill Burr’s 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error.

*By Robert McMillan*

Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.
• “152 steps to Cyber Security” (Reeder et al. 2017): Security experts cannot agree on 3 most important behaviours
• Stobert & Biddle 2016: Security experts don’t follow their own advice on password management … and take risks they decry in users
• Don’t get me started on CAPTCHAs and self-phishing … (more later)
Problem 2: Productivity-destroying security

“Sticky plaster security” gets in the way and zaps
- Time
- Attention
- Goodwill
David Rosenthal @MakeYourselfNrd

We started doing training a long time ago. Still get phished on occasion like everyone, but now everyone is afraid of any 3rd party link 😞

7:26 am - 17 Aug 2017

David Rosenthal @MakeYourselfNrd · Aug 17

Replying to @MakeYourselfNrd @ajohnsocyber @SwiftOnSecurity

Response rate on some 3rd party survey tools went down drastically after training started. Even with fully branded and well written comms. 😞
"About 50 of you so far marked this message coming from [subcontractor] as phishing"

Email from HR department in a company with around 600 employees that had hired a well-known, expensive supplier to conduct employee surveys.

NCSC guidance on measures to reduce phishing
https://www.ncsc.gov.uk/phishing
Problem 3: Negative security

- Security experts try to motivate behaviour change through fear

Another example: Devil's in your details https://www.youtube.com/watch?v=Ugl8bmZF9Pc
FUD is damaging – not just to users

“FUD provides a steady stream of factoids (e.g. raw number of malware samples, activity on underground markets, or the number of users who will hand over their password for a bar of chocolate), the effect of which is to persuade us that things are bad and constantly getting worse. […] reliance on factoids leads government and industry to spend wastefully and researchers to focus on the wrong questions.”

Problem 4: Paternalistic security

• Many studies attempting to ‘nudge’ users towards security
• Based on behavioural economics, but overlooks key aspects of that theory – the nudgee has to want goal and agree on way of getting there …
Problem 5: Annoying security

- Disruptive, creating stress, anger, other negative emotions
WE HAVE TWO RENTAL CARS LEFT. ONE IS THE MURDER CAR. BUT DON'T LET THE NAME SCARE YOU! IT'S DEFINITELY HAUNTED, BUT MOST DRIVERS DON'T GET MURDERED. MAYBE ONE IN SIX.

THE OTHER IS A REGULAR SEDAN. BUT IT HAS A GPS THAT'S STUCK TRYING TO NAVIGATE TO SEATTLE, AND YOU CAN'T TURN IT OFF.

...I CAN IGNORE IT, RIGHT? THAT'S FINE.

TURN LEFT
RECALCULATING
MAKING A U-TURN
RECALCULATING
TURN RIGHT
RECALCULATING

BACK ALREADY?
WE'LL TAKE THE MURDER CAR.

POPULAR CHOICE.
Problem 6: “Security awareness”
So - how do we fix security?

1. Make security possible - usability is essential, not a luxury.
2. Security education cannot fix security people don’t want.
3. Transforming user behaviour requires serious long-term work.
4. All the good guys need to work together, not against each other.
Back to the future – the ‘Kerckhoffs Test’

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Positive Security that people want

- From ‘freedom from’ (threats) to ‘freedom to’ (do the things people want)
  - putting user goals and values first
  - positive language and genuine enablement
- Employ basic usability principles and methods
  - commitment to understanding performance and employing metrics
  - inclusive design
Everyday Security
Lizzie Coles Kemp
2018-04-23 & © RHUL & individual contributors 2018
Published by Royal Holloway University of London
Creative Securities Book 3
collectivesecurities.org
Creative Security Engagement Methods

https://www.trespass-project.eu/
Awareness Maturity Curve

- Safe behavior
- Acceptance
- Implementation (skills / abilities)
- Conviction (positive perception / attitude)
- Understanding / Knowledge
- Sensitizing
- Information

Investment (Time, budget, human resources)

Personal Commitment

Covered by extra commitment of the company

Covered by ISO 27001: A.7.2.2 Information security awareness, education and training

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
Fogg Behavior Model

B = mat
at the same moment

High Motivation

Trigger at this point & behavior happens

Low Motivation

Activation Threshold

Hard to Do

ability

Easy to Do
“Culture eats strategy for breakfast.” Peter Drucker

“Productivity eats security for breakfast, lunch and dinner.”
Angela + her research team

“Trust and collaboration ... are necessary for effective cybersecurity.”

Compliance is not enough

Learning from medicine

**Adherence (compliance):** Patient follows the plan set our by professional. Less than half of patients comply.

**Concordance:** Patient and professional agree the most appropriate treatment plan – clarification of goals, joint responsibility. More than half of patients stick to agreed plan.
Levels of Security Maturity

Level 5: Champions security to others and challenges breaches in their environment.
Level 4: Has internalised the intent of the policy and adopts good security practices even when not specifically required to.
Level 3: Understands that a policy exists and follows it by rote.
Level 2: Follows security policy only when forced to do so by external controls.
Level 1: Is not engaged with security in any capacity.
Security Dialogues

• Ashenden & Lawrence (2016)
• 3 x 3-day workshops, with 18 security professionals in total
• First learnt why developer acted the way they did
• Then: skills to engage and support staff
  • conflict resolution skills from counselling
  • social market theories of exchange and influence
  • how to design behaviour change interventions
Security training for security experts

1. Change of attitude - “we’re here to help you do what you want to do, securely”.
3. Learn how to communicate, negotiate, become trustworthy.
4. Know how to test for effectiveness of security measures and strive for continuous improvement.
5. Use of fear tactics or user-bashing results in an automatic fail.