

The True Cost of Unusable Security

M. Angela Sasse

Professor of Human-Centred Technology,

Head of Information Security Research

Department of Computer Science

University College London, UK

a.sasse@cs.ucl.ac.uk

www.ucl.cs.ac.uk/staff/A.Sasse

History

- Study on escalating cost of password resets at BT
 - too high workload
 - leads to shortcut security mechanisms
 - Users don't understand threats and risks
- Also 1999: Whitten & Tygar *"Why Johnny can't encrypt"*

USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect

access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that

do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

ANNE ADAMS AND
MARTINA ANGELA SASSE

Adams & Sasse CACM 1999

What Has Happened Over The Past Decade?

– Lots:

- ACM SOUPS (Symposium on Usable Security and Privacy) since 2004
- SHB (Security & Human Behaviour) since 2008
- Papers in CHI, CCS, Usenix, NSPW ...
- Books: Cranor & Garfinkel, Shostack, Lacey
- University modules usable security
- White Paper on *Human Vulnerabilities in Security Systems (UK)* 2007
- US National Academy of Sciences Workshop on *Usable Security and Privacy* 2009

And - has it made security (more) usable?

- Nielsen (2000) said that biometrics are highly usable and would replace passwords – hasn't happened.
- Schneier (2000) and Gates (2004) predicted that passwords would become obsolete
- Didn't happen. Why?

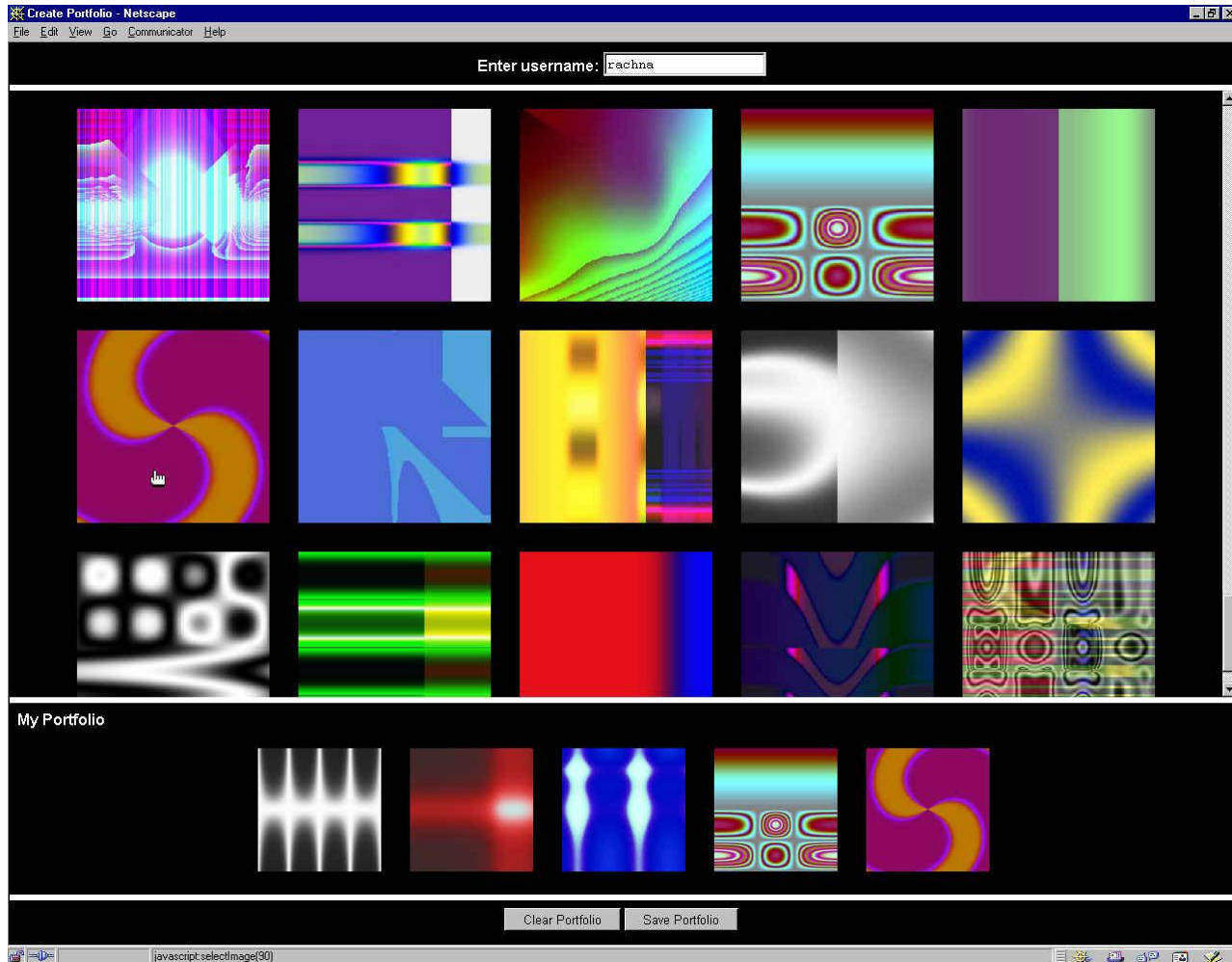
Instead: passwords are still bugging users

- 6-8 passwords per employee within organisation, despite SSO
- Time spent constructing & entering passwords still significant
- Externalisation (writing down) of passwords and extensive re-use (see also *Florencio & Herley 2007*)
- Increasing number of self-service re-sets
- New layers of credentials added (e.g. challenge questions)

P. Inglesant & M. A. Sasse: The True Cost of Unusable Password Policies. Procs ACM CHI 2010.

Graphical Passwords: Déjà Vu

Dhamija & Perrig 2002



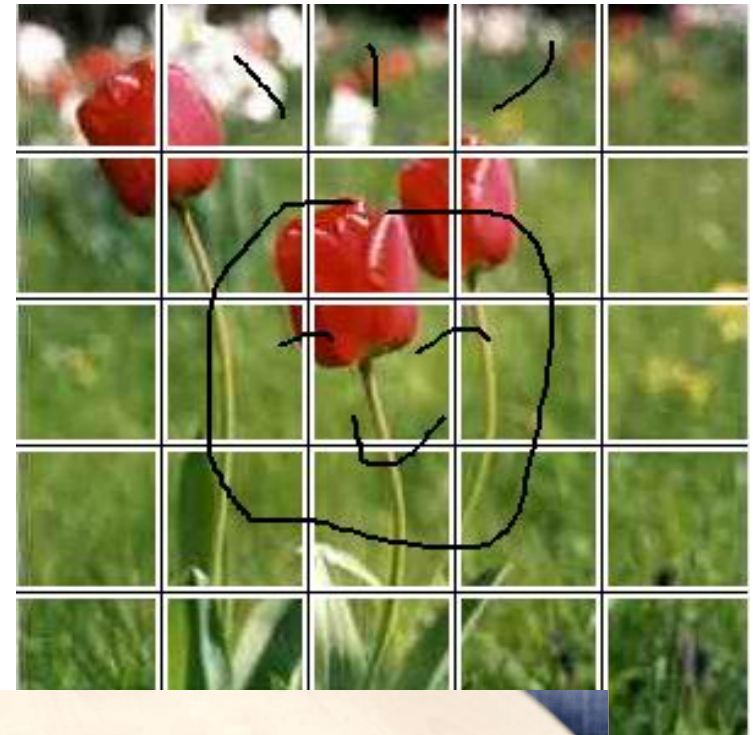
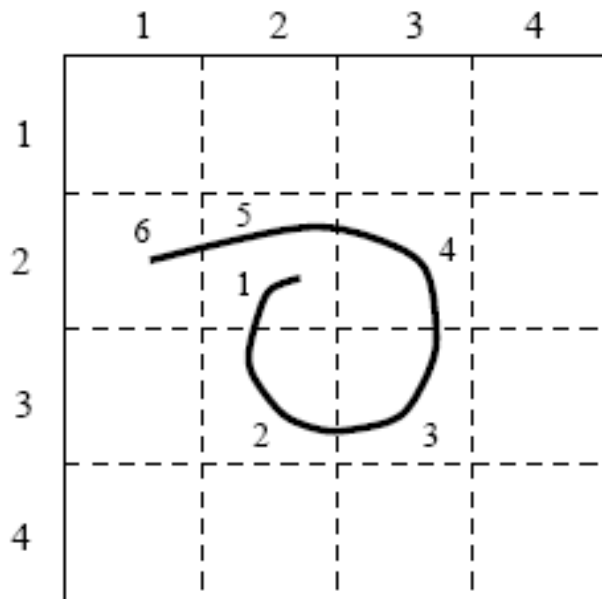
Persuasive Cued Clickpoints

- 1 click-point per image
- Next image determined
- by current click-point

Chiasson et al, HCI 2008



Draw-a-Secret & BDAS



Yan et. al



9	8	1	7	5
0	4	3	1	2
8	7	0	4	3
1	8	5	6	2
9	2	9	8	4

- Personal Identification Pattern
- User selects pattern from grid (min. 5 x 5)
- Numbers displayed on grid
- User reads PIN off grid displayed and enters one-time PIN via keypad into sales unit/ATM/home PC.

www.gridsure.com

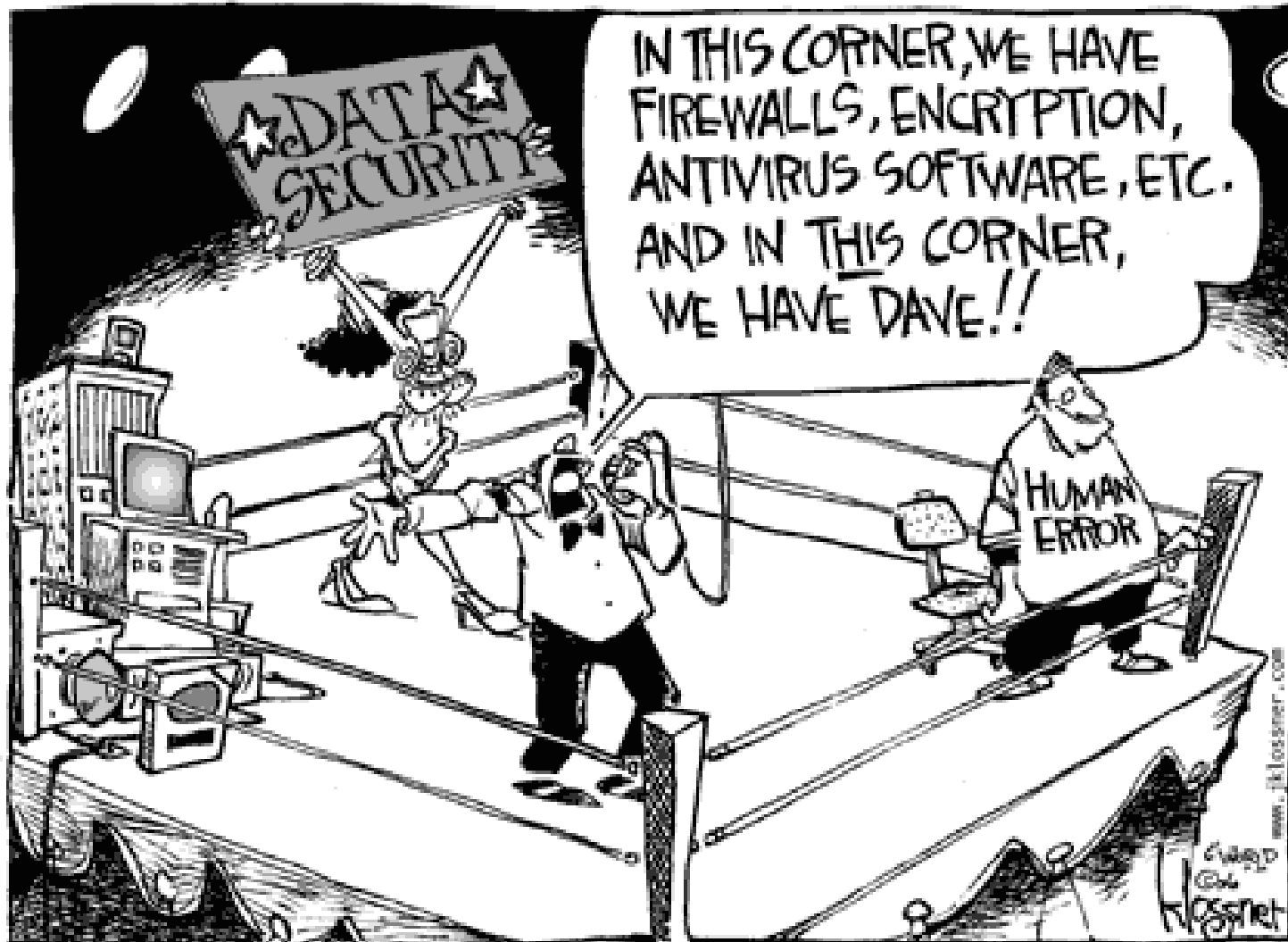
More ‘usable’ authentication ...

- Authentication via Rorschach inkblot tests
- Singing your password (Reynaud et al., NSPW 2007)
- Thinking your password (free EEG thrown in - Thorpe et al., NSPW 2005)
- Schneier: fMRI would be cool
- More biometrics (some more dubious than others)
- Ringing up your friends in the middle of the night to provide you with previously entrusted re-set codes (Microsoft)

Meanwhile, in the real world ...

- Companies selling alternative authentication mechanisms go bust:
 - Vidoop
 - Pay-by-touch
- Authentication problems continue, with noticable impact on productivity and security
 - Expensive helpdesk re-sets, or easy-but-vulnerable re-sets
 - Weak passwords, extensive password re-use, stored in files and email folders

What's wrong with usable security thinking?



- Shallow understanding of usability:
 - “Better user interfaces” to security tools, or replacing existing security controls with “more usable” alternatives
 - Failure to consider fundamental usability constraints: user goals and values, tasks and workflows, physical and social context
- Old-school security thinking:
 - Treating humans as components that can be controlled by policy (if only they can understand how to use security controls properly)

Finally, people are waking up to the cost ...

- *“Security people value users’ time at zero.”*
(Herley NSPW 2009)
- *“If only security managers understood the true costs for users and the organisation, they would set policies differently”* (Inglesant & Sasse, CHI 2010)
- *“CAPTCHAs waste 17 years of human effort every day”* (David Pogue, Scientific American, March 2012)

The burden on users



- 'A tale of two laptops'
- Spending 30 mins/day logging in
- Spending 2 hours/month updating passwords

PAS

... leads to undermining security



- Browser-stored passwords, password managers
- Mouse-jigglers and dipping birds to disable screen locks
- Copying and emailing access-controlled documents
-



Tasks

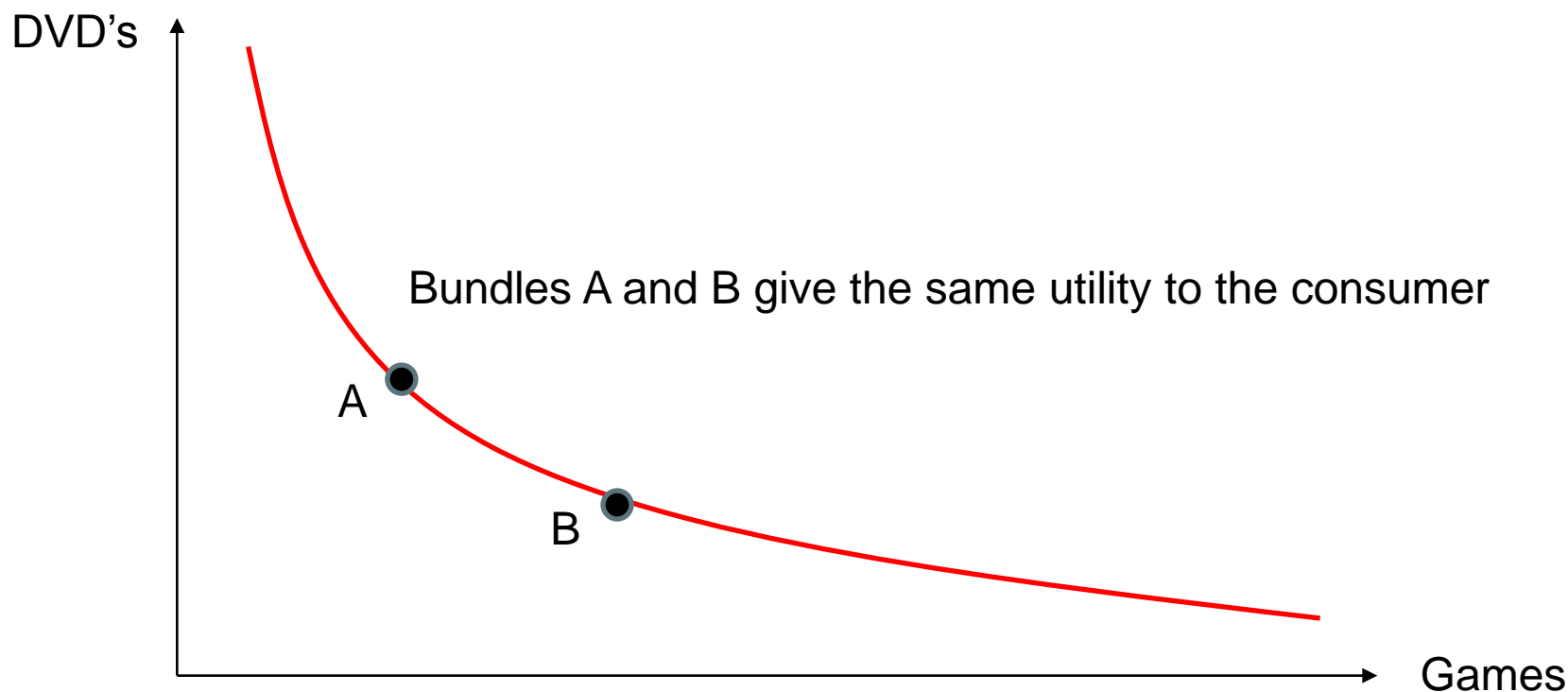
- Security is secondary task
 - should be designed to fit into primary task (and user capabilities)
 - primary task (which is part of workflow) should set performance requirements
- Current situation:
 - security tasks are “obstacles” on the completion to primary tasks
 - Workload and complexity pushed on users
 - Users faced with conflicting primary/security task requirements

Economic Concepts: Preference/Indifference

- With respect to a set of goods A and B a person can:
 - Strongly prefer A to B
 - Weakly prefer A to B
 - Be indifferent between A and B
- The behaviour of a person can (to some extent) be predicted from these preferences

The Indifference Curve

- Essentially shows at what rate an entity is willing to trade between two goods



Economic concepts: Trade-Offs

- We understand the trade-offs a consumer makes when purchasing goods.
 - A trade-off occurs where increasing the amount of one good available decreases the amount of another
- Trade-offs in economics are very well understood
- Trade-offs exist in security, but are often not well understood
 - e.g. Confidentiality and Availability

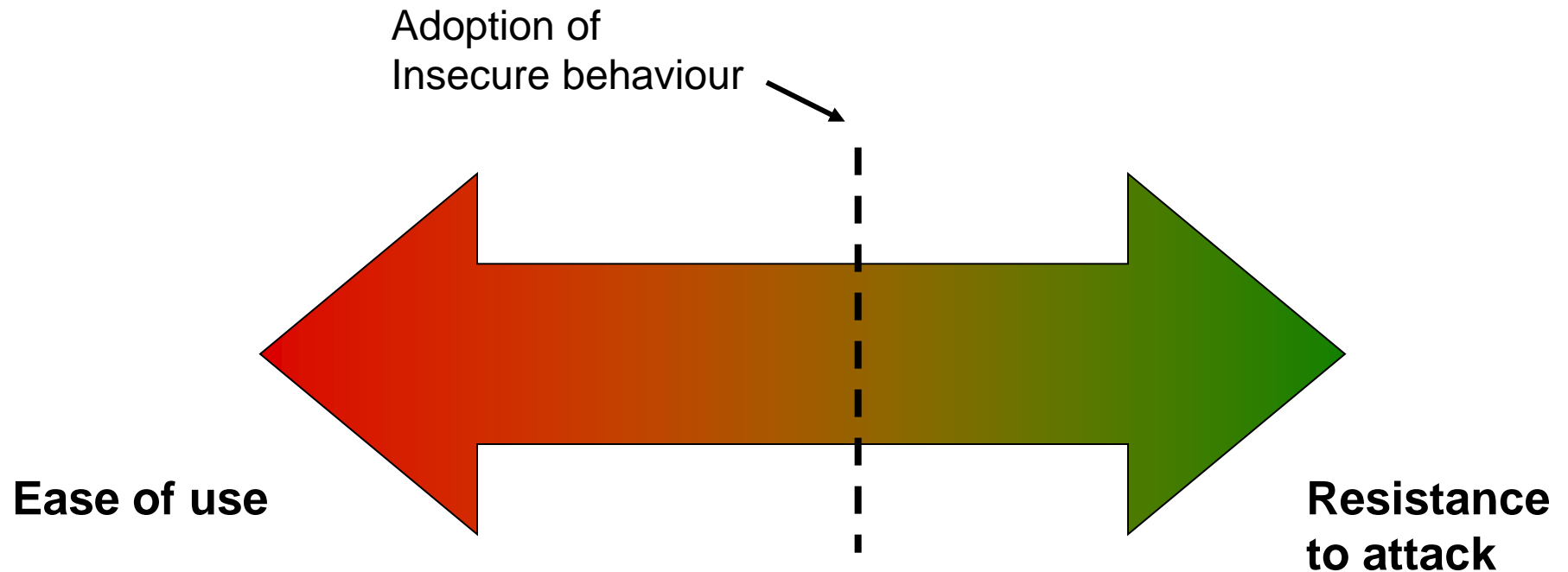
Users trade-offs in security

- Perceived effort
 - Physical workload
 - Mental workload
- Interference with primary task
 - reduction in personal productivity
 - reduction in organisational productivity
- Failure costs
- Risk to themselves (incl. sanctions)
- Other risks to organisation
 - Financial loss
 - Reputation
- Perceived likelihood of these occurring

Longer-term impact - examples

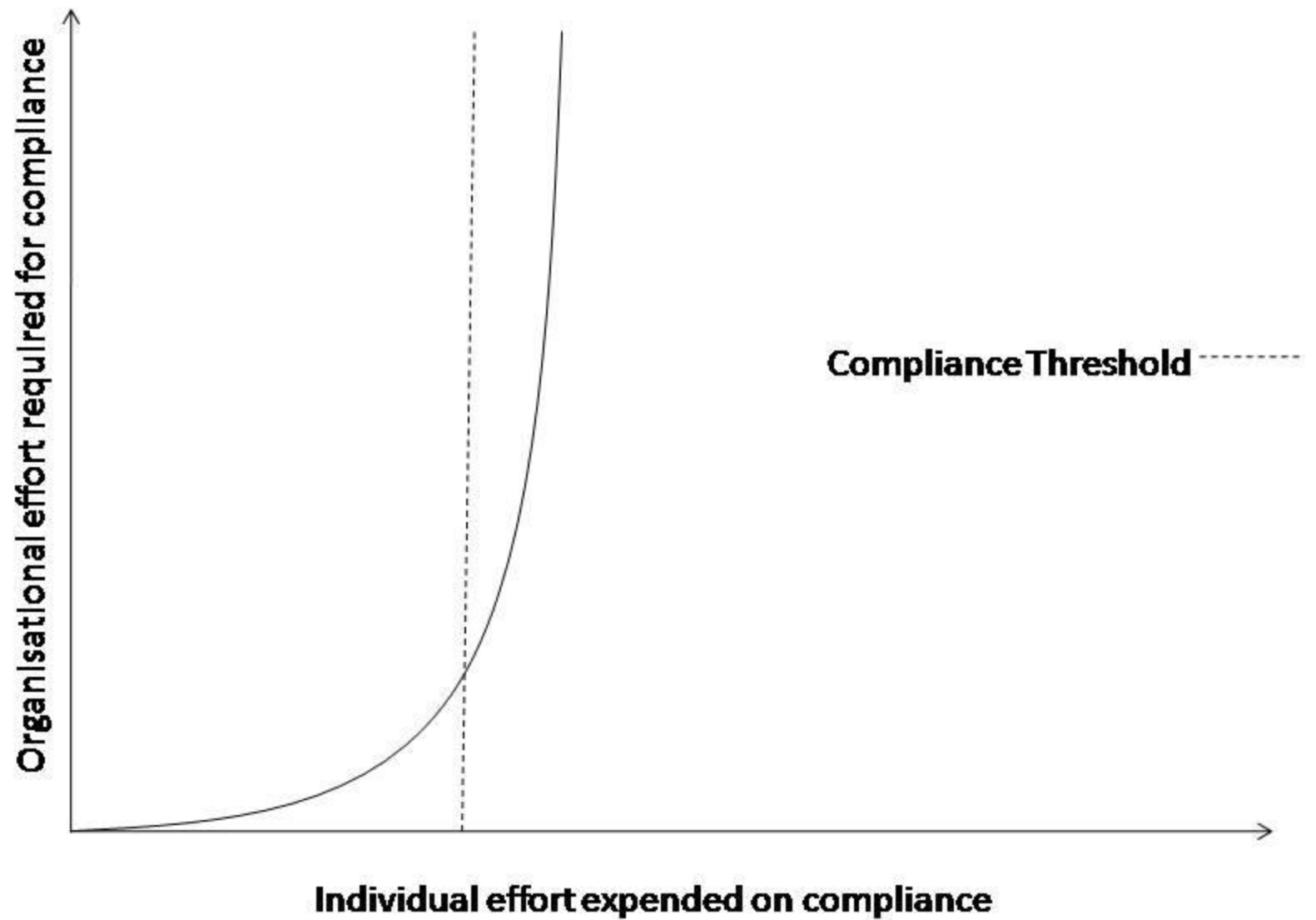
- Not answering email from home
- Not having/taking a company laptop
- Not collaborating with externals/other organisations

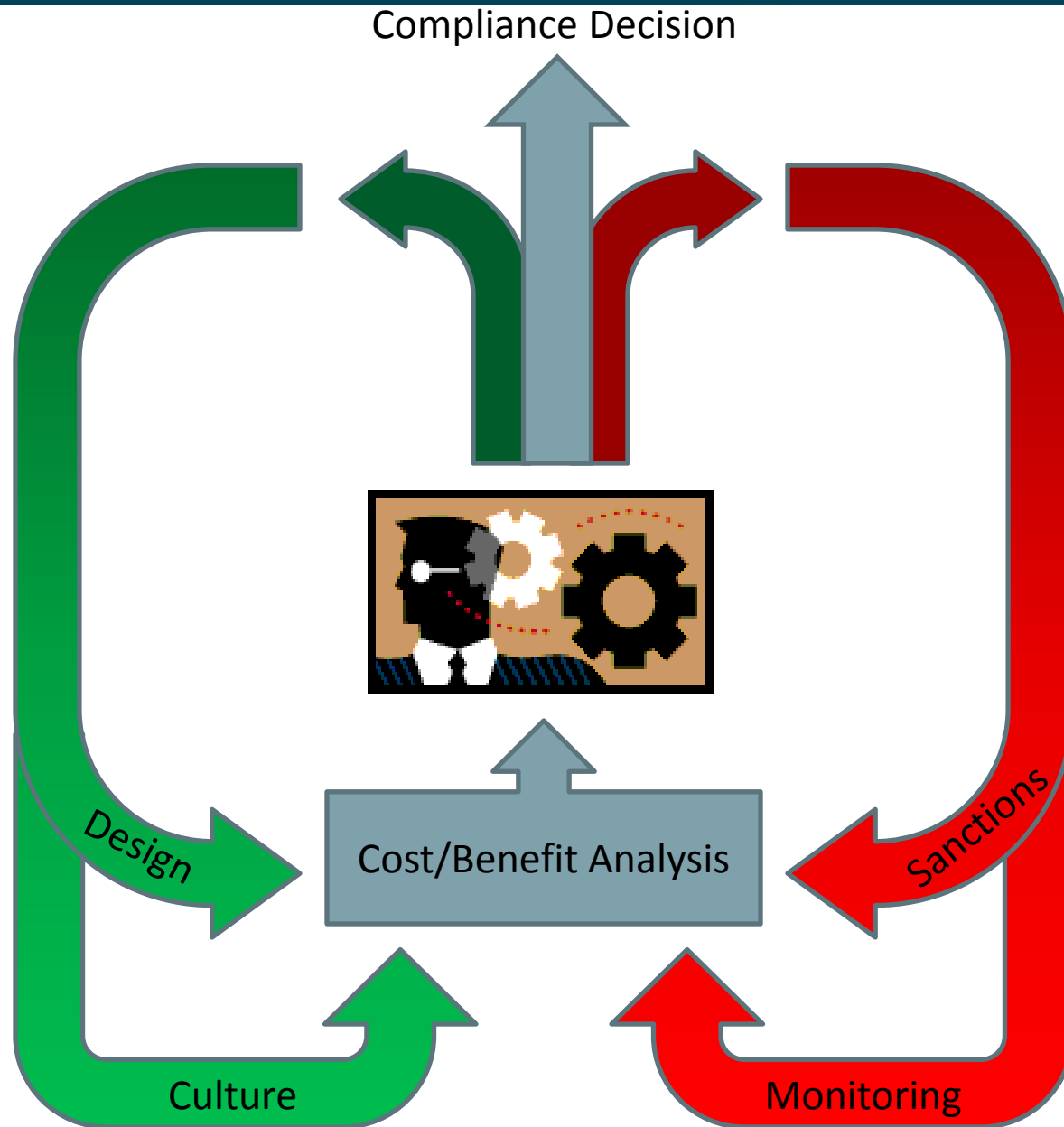
The Operating Point



The Compliance Budget

- Explains how employees make compliance decisions
- Based on interviews with employees and security managers in organisations
- Extracted cost/benefits of individual security tasks (passwords, encryption, patches)
- Perceived cost to the user more important than measurable cost
- Perceived load accumulates over tasks ...





Cost of security measures

F. Pallas: The New Economics of Information Security. PhD thesis TU Berlin 2008

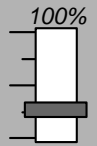
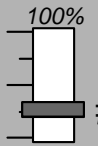
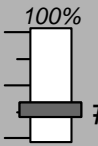
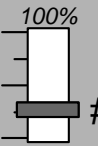
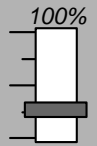
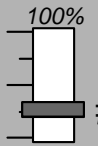
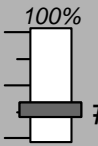
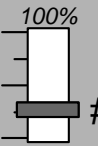
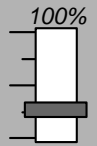
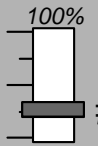
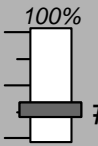
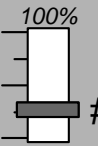
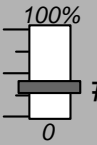
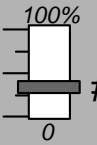
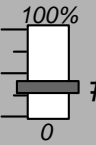
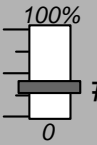
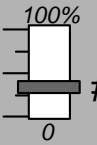
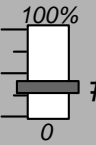
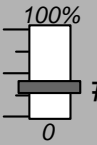
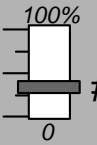
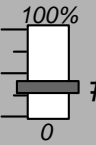
Meta-Measure	Initial Costs (once)	Enforcem. Costs	Loss from non-compliance
Architect. Means	high	none / negligible	none / negligible
Formal Rules	low	high	high
Informal Rules	medium	low (spont.)	high

Need to Target Security Decision-Makers

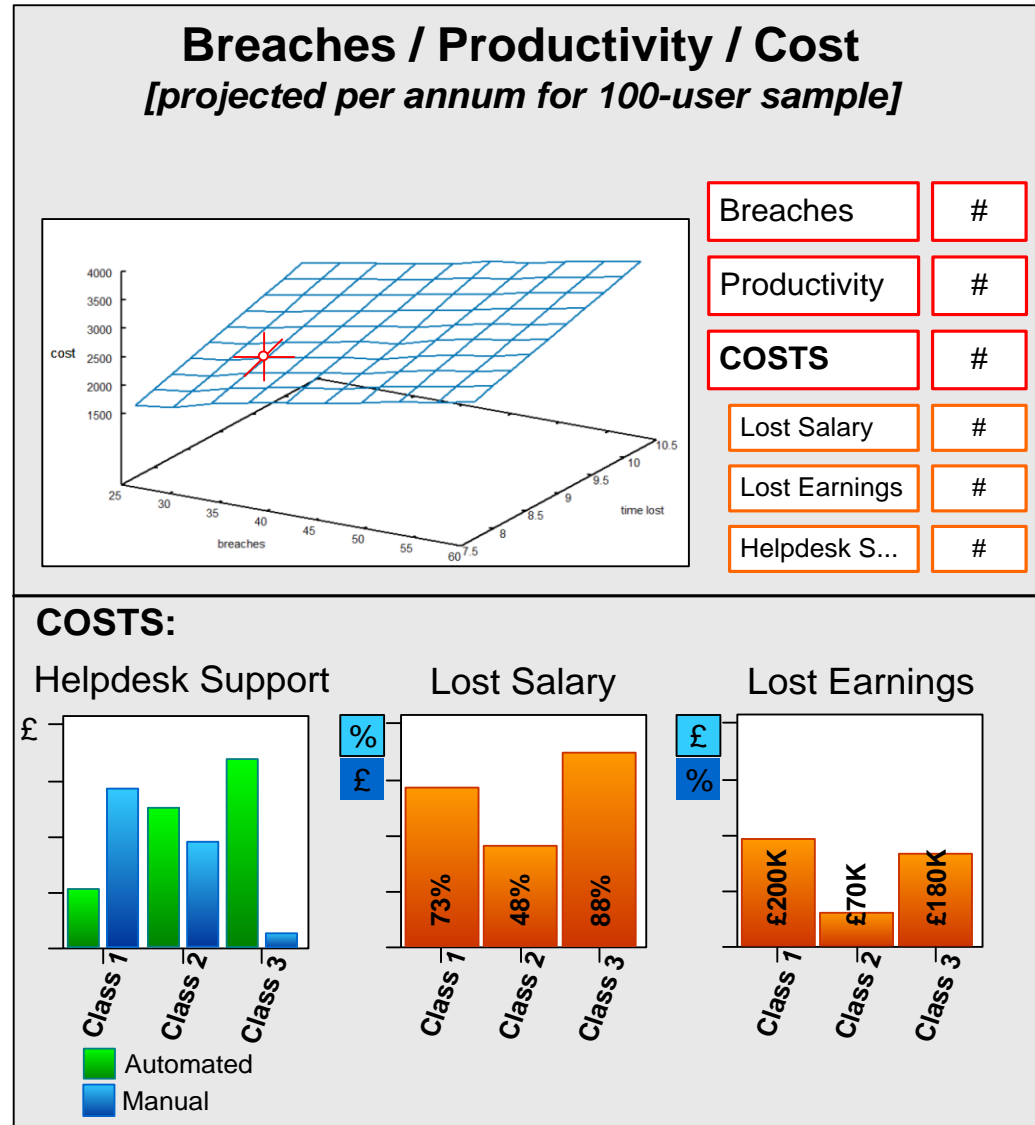
- CISOs are key decision-makers
- Q: Why is it so hard to get CISOs interested in usable security?
- A: Because they make their own trade-offs: security investment cost vs. risk reduction

... and they forget impact on productivity

*S. Parkin, A. Van Morsel, P. Inglesant & M. A. Sasse:
A Stealth Approach to
Usable Security.
Procs. NSPW 2010*

Policy Properties	Support Properties	User Properties								
Select User Class ... ▼		Class 1								
Class Name:		<input type="text"/>								
Average Salary:		GBP ▼ <input type="text"/>								
Average Projected Annual Earnings:		USD ▼ <input type="text"/>								
Working Pattern: <table border="1"> <thead> <tr> <th>Home</th> <th>Office</th> <th>Public</th> <th>In Transit</th> </tr> </thead> <tbody> <tr> <td> 100%  #% 0 </td> <td> 100%  #% 0 </td> <td> 100%  #% 0 </td> <td> 100%  #% 0 </td> </tr> </tbody> </table>			Home	Office	Public	In Transit	100%  #% 0	100%  #% 0	100%  #% 0	100%  #% 0
Home	Office	Public	In Transit							
100%  #% 0	100%  #% 0	100%  #% 0	100%  #% 0							
User Distribution: <table border="1"> <thead> <tr> <th>% ▼</th> <th>Class 1</th> <th>Class 2</th> <th>Class 3</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td> 100%  # 0 </td> <td> 100%  # 0 </td> <td> 100%  # 0 </td> </tr> </tbody> </table>			% ▼	Class 1	Class 2	Class 3	<input type="text"/>	100%  # 0	100%  # 0	100%  # 0
% ▼	Class 1	Class 2	Class 3							
<input type="text"/>	100%  # 0	100%  # 0	100%  # 0							

Dashboard interface for CISOs



Conclusions

- User compliance underpins virtually all security systems
- Pushing workload on users reduces
 - personal and organisational productivity
 - Security compliance
- The paths forward
 - Security decision-making informed by economic thinking and empirical evidence
 - Integrating security into business processes → requirements and software engineering

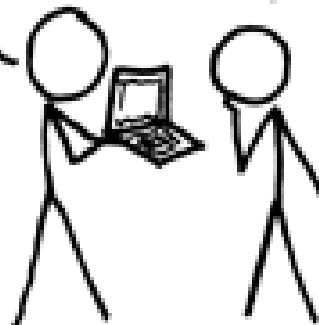
Questions?

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.

