University of BRISTOL

CyBOK

Cyber Security Body of Knowledge: Human Factors

Awais Rashid
Bristol Cyber Security Group
University of Bristol, UK

bristol.ac.uk

University of BRISTOL

CyBOK

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

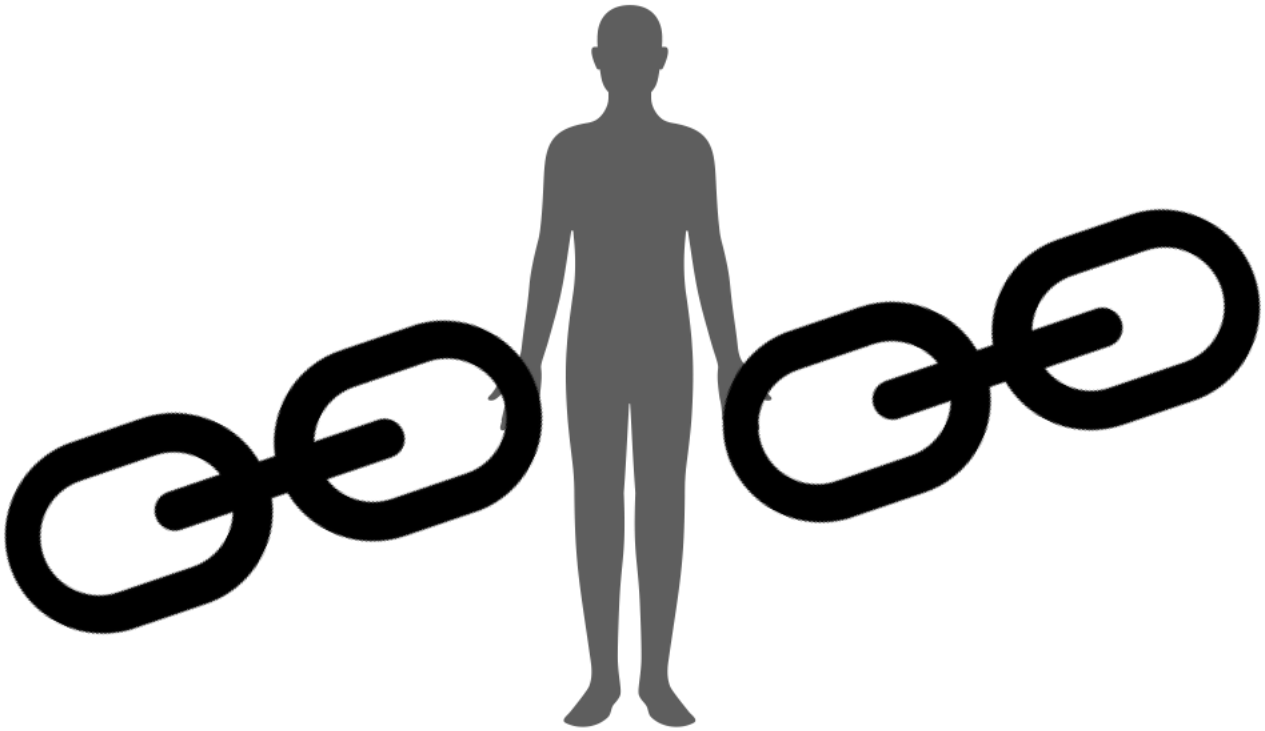
bristol.ac.uk

CyBOK

Less that 0.1% of email is end-to-end encrypted!

A. Whitten and J. D. Tygar, “Why johnny can’t encrypt: A usability evaluation of pgp 5.0.” in USENIX Security Symposium, vol. 348, 1999.

CyBOK



bristol.ac.uk

CyBOK

Users are not the Enemy!

A. Adams and M. A. Sasse, “Users are not the enemy,” Communications of the ACM, vol. 42, no. 12, pp. 40–46, 1999.

CyBOK

Fit the human to the task

CyBOK

Fit the task to the human

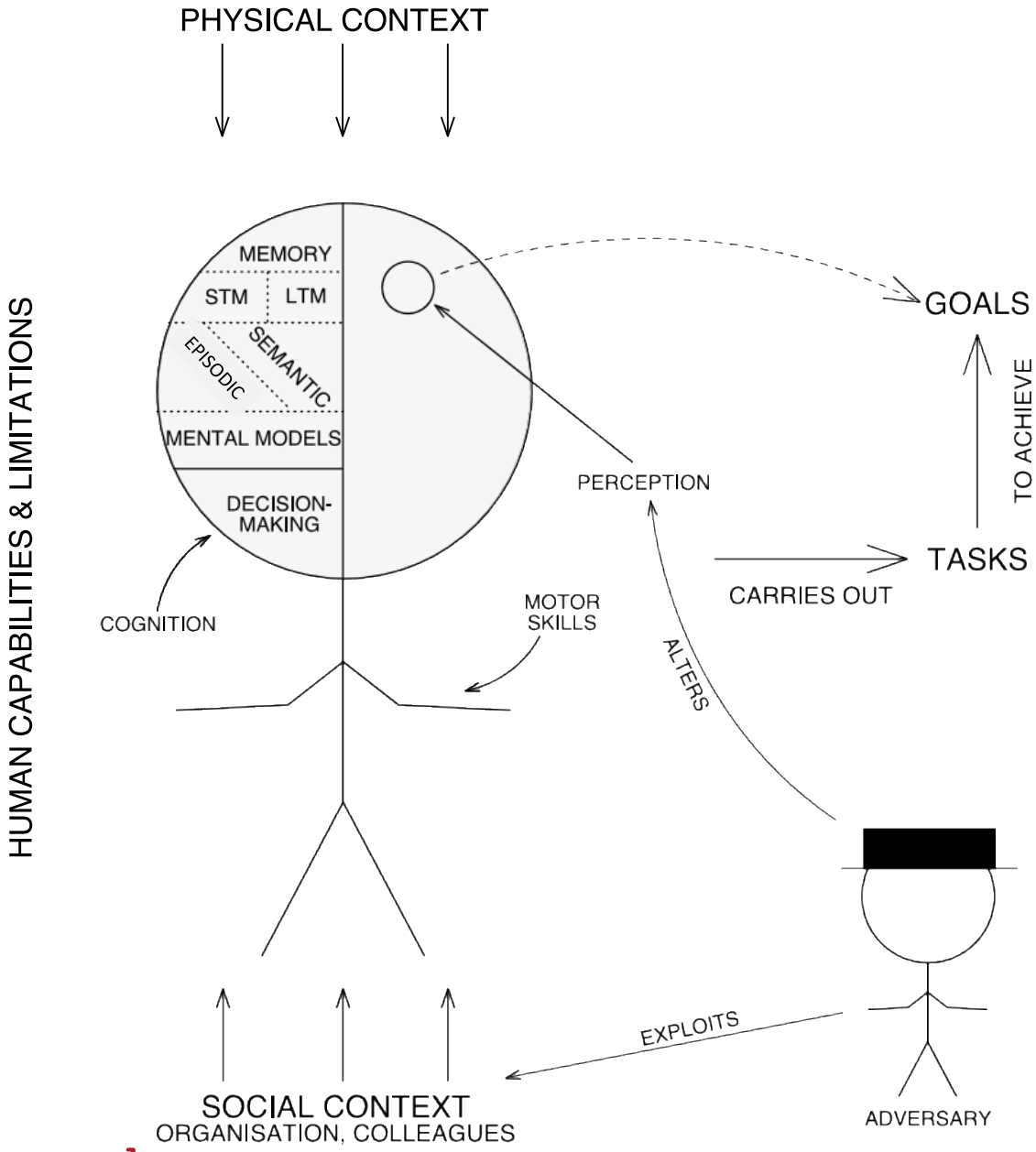
CyBOK

Security has to be usable

Effectiveness: Can users achieve their goals?

Efficiency: What resources are expended to do so?

Satisfaction: What is the level of comfort and acceptability for users?

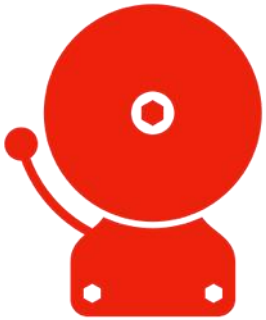


CyBOK

bristol.ac.uk

CyBOK

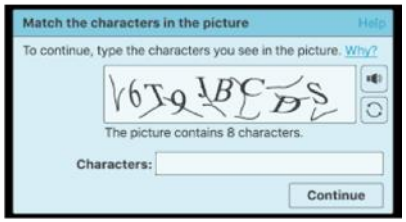
Human Capabilities and Limitations



Alarm Fatigue

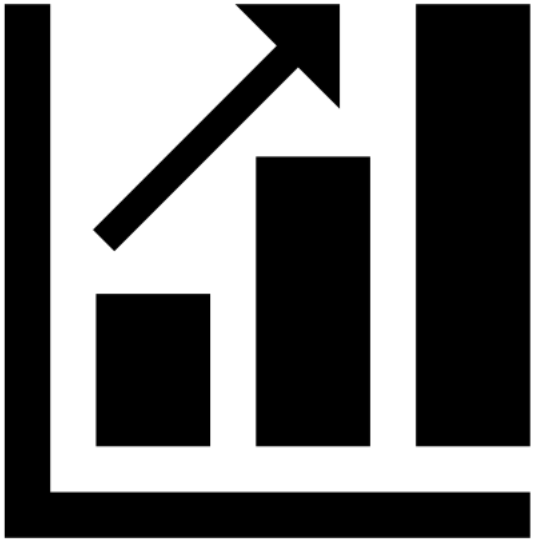
STM vs. LTM

Strength Meters



CAPTCHA

CyBOK



VS.

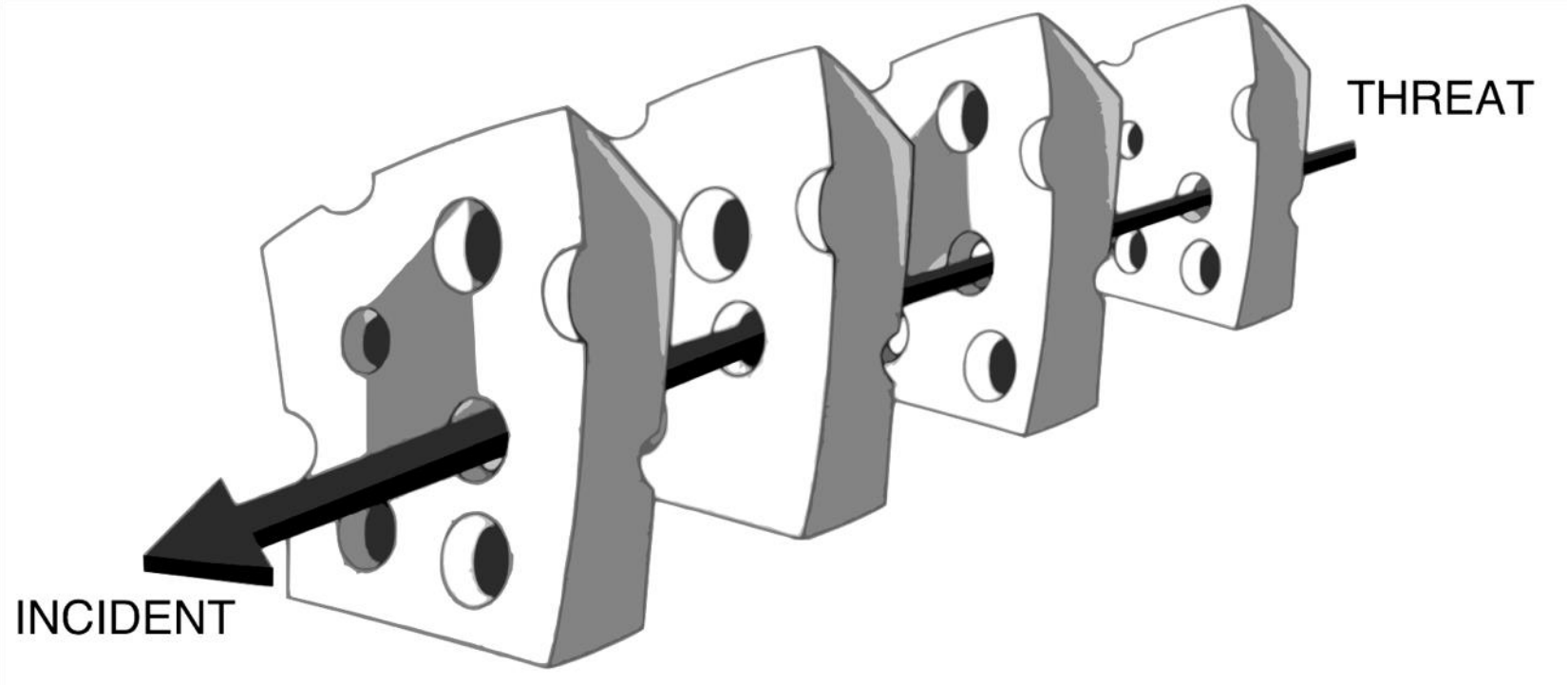
bristol.ac.uk

CyBOK

Compliance Fatigue

CyBOK

Latent Design Conditions



CyBOK

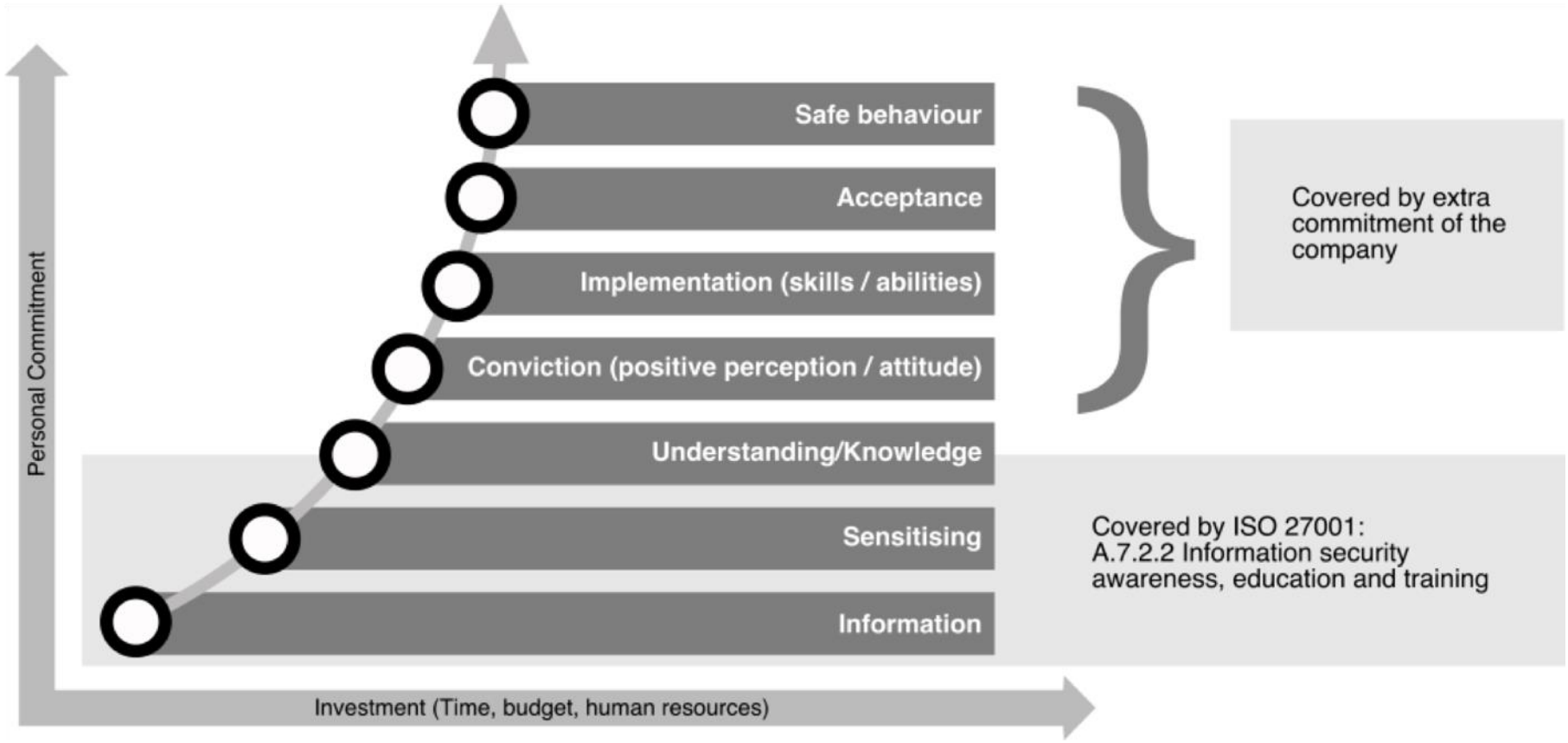
“Never give an order that can’t be obeyed”

General MacArthur

Never issue a security policy that cannot be followed

CyBOK

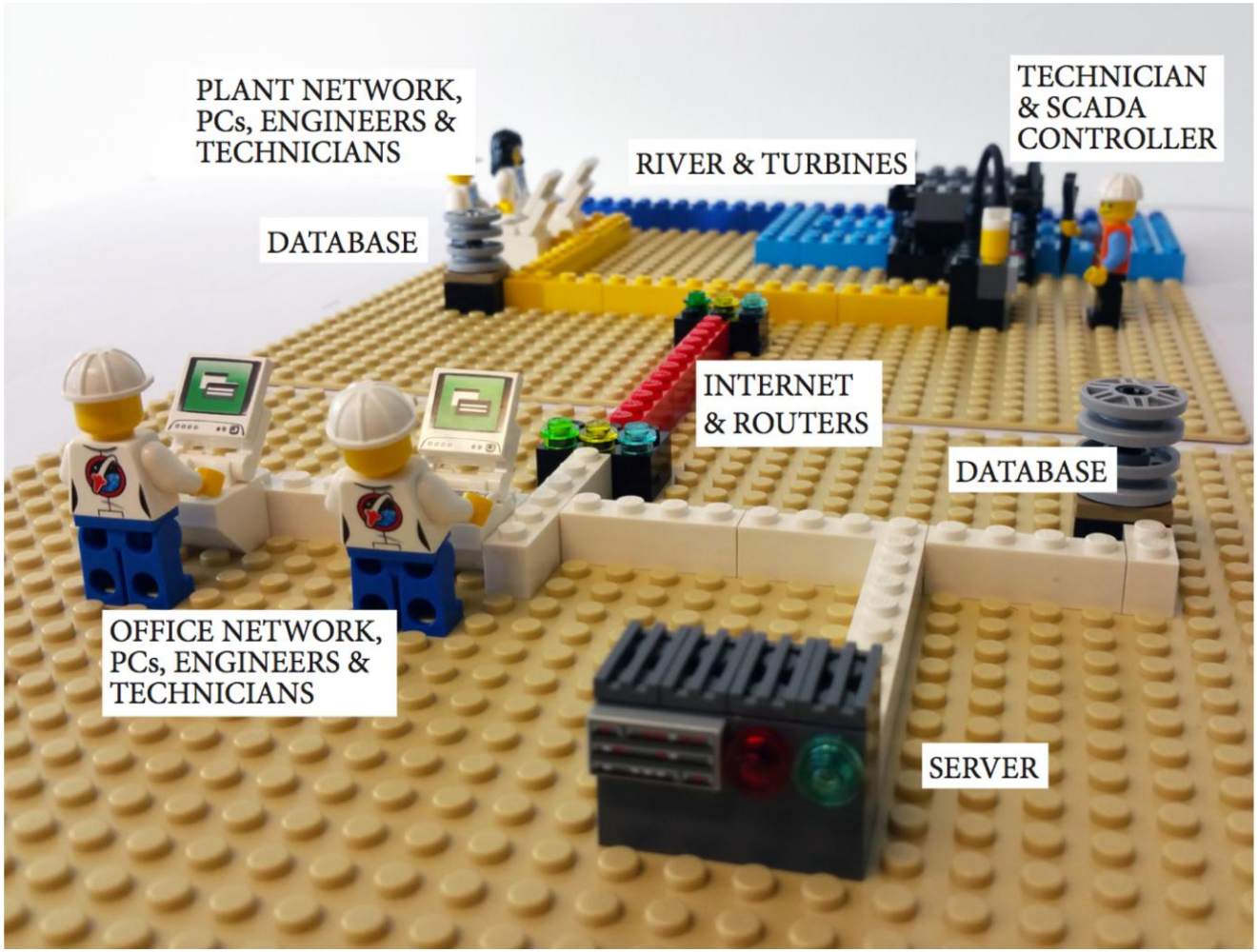
Awareness and education



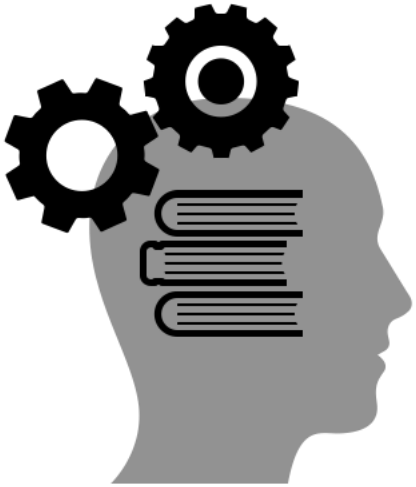
CyBOK

bristol.ac.uk

CyBOK


PLANT NETWORK, PCs, ENGINEERS & TECHNICIANS
TECHNICIAN & SCADA CONTROLLER
RIVER & TURBINES
DATABASE
INTERNET & ROUTERS
DATABASE
OFFICE NETWORK, PCs, ENGINEERS & TECHNICIANS
SERVER

CyBOK



Mental models of cyber security and risks

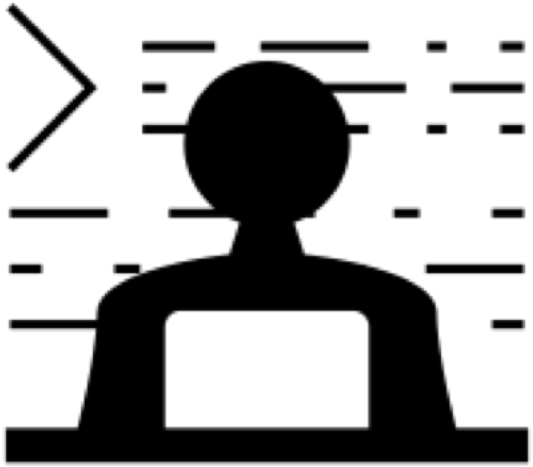
bristol.ac.uk

CyBOK

FUD

bristol.ac.uk

CyBOK

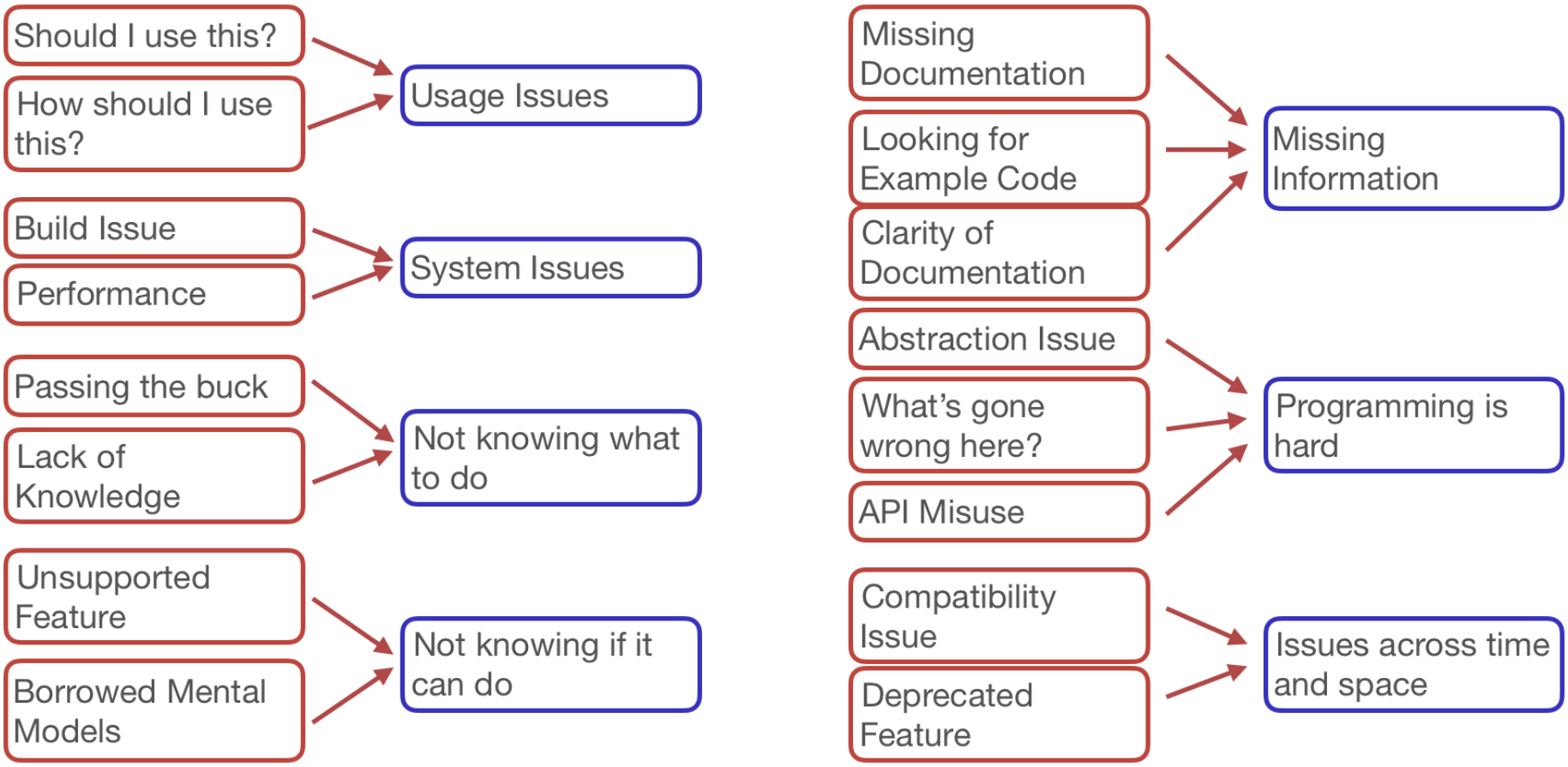


What about developers?

bristol.ac.uk

CyBOK

What Usability Issues Do Developers Face?



bristol.ac.uk

N. Patnaik, J. Hallett, and A. Rashid, "Usability smells: An analysis of developers' struggle with crypto libraries," in Fifteenth Symposium on Usable Privacy and Security (SOUPS), Santa Clara, USA. USENIX Association, 2019.

CyBOK

Developers are Not the Enemy! The Need for Usable Security APIs

Matthew Green and Matthew Smith
IEEE Security & Privacy 14(5), Sept.-Oct. 2016.

CyBOK

Principles for Usability of Crypto APIs

Abstract: Integrate cryptographic functionality into standard APIs so regular developers do not have to interact with cryptographic APIs in the first place.

Powerful: Sufficiently powerful to satisfy both security and non-security requirements.

Comprehensible: Easy to learn, even without cryptographic expertise.

Ergonomic: Don’t break the developer’s paradigm.

Intuitive: Easy to use, even without documentation.

CyBOK

Principles for Usability of Crypto APIs

Failing: Hard to misuse. Incorrect use should lead to visible errors.

Safe: Defaults should be safe and never ambiguous.

Testable: Testing mode. If developers need to run tests they can reduce the security for convenience.

Readable: Easy to read and maintain code that uses it/Updatability.

Explained: Assist with/handle end-user interaction, and provide error messages where possible.

CyBOK

Usability Smells: An Analysis of Developers' Struggle With Crypto Libraries

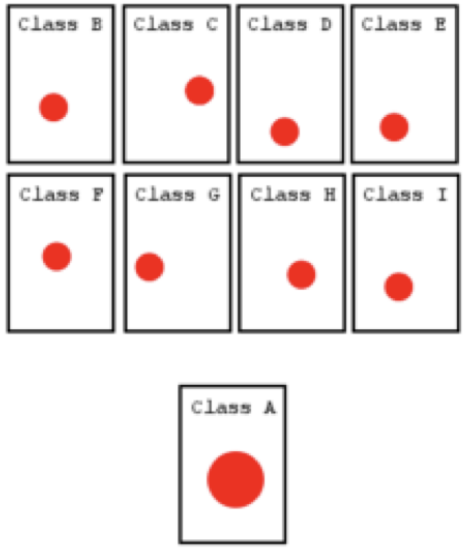
Nikhil Patnaik, Joseph Hallett and Awais Rashid
Proceedings of 15th International Symposium on Usable Privacy and Security (SOUPS) 2019.

bristol.ac.uk

CyBOK

Fowler's Shotgun Surgery

"You whiff this when every time you make a kind of change, you have to make a lot of little changes to a lot of different classes. When the changes are all over the place, they are hard to find, and it's easy to miss an important change" – Definition of Shotgun Surgery



CyBOK

1 Need a super-sleuth

You whiff this when documentation is missing, unclear or there is a lack of example code pertaining to how to use the library.

2 Confusion Reigns

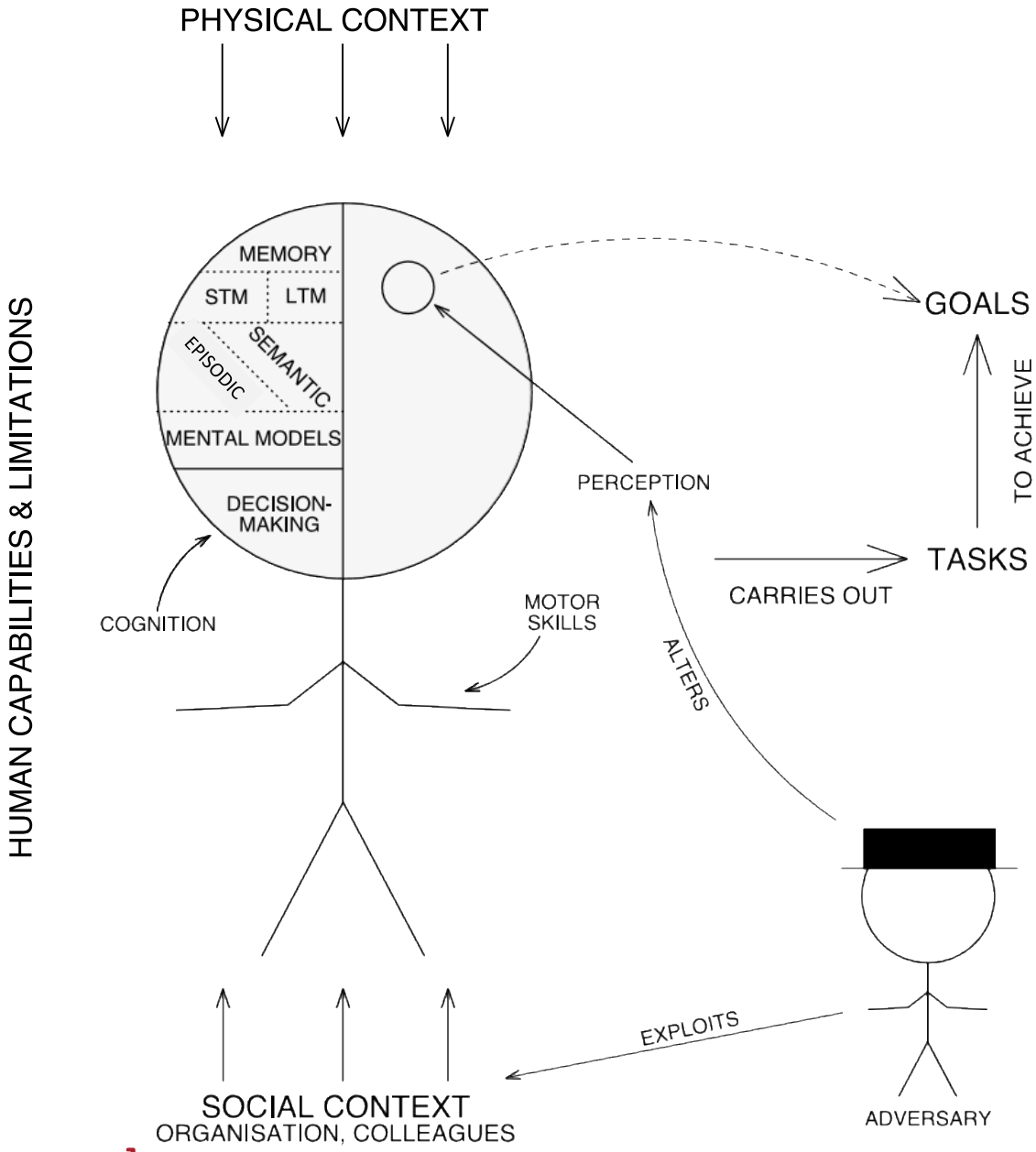
You can catch a whiff of this when developers are designing and prototyping their programs —they are trying to decide whether this is the right library to use and how to start using it.

3 Needs a post-mortem

The developer has used the library but something has gone wrong. Either they have used the library incorrectly or they are struggling to work out if it is an issue with the library itself.

4 Doesn't Play Well With Others

This smell occurs when the library won't build, won't integrate with other libraries and build systems, and is a resource hog without providing a clear explanation why.



CyBOK

bristol.ac.uk

CyBOK

Fit the task to the human