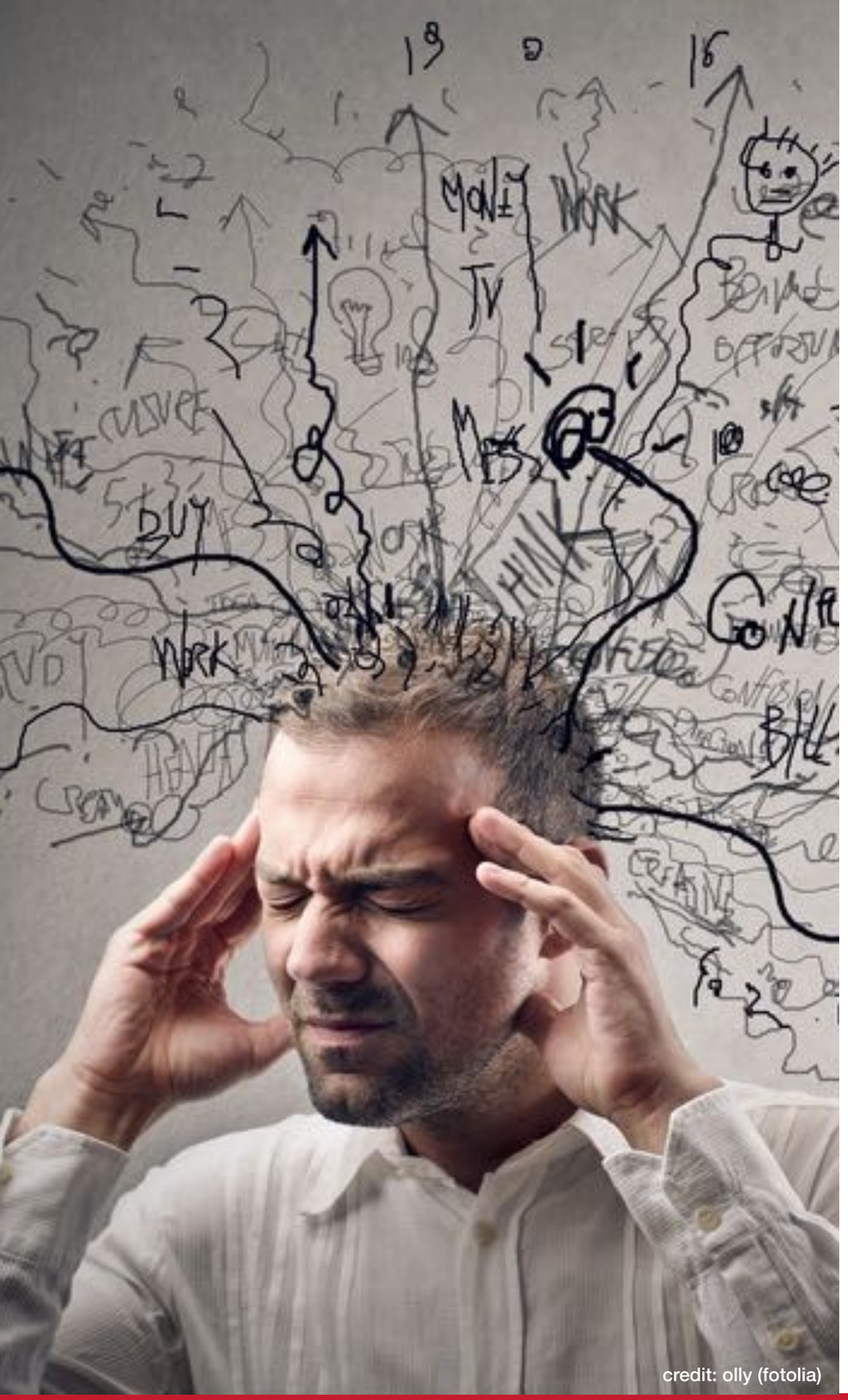
Security Behaviours

COMS30038 Lecture 8 - Error in Practice

Dr Ramokapane

University of BRISTOL

Bristol Cyber Security Group



Quick Inclusive Security Recap

Usability focuses on *ease* — fitting the task to the human.

Accessibility ensures *ability* — enabling interaction for everyone.

Inclusivity ensures *equity* — designing systems that protect and empower all users fairly.

Usability ≠ Universality
Security that works for some users may fail or endanger others.

Exclusion is a Latent Failure
Designs that ignore diversity create hidden vulnerabilities.

Accessibility Enables, Inclusivity Empowers
Accessible systems remove barriers; inclusive systems build equity and trust.

Diversity is a Security Control
Different perspectives reveal different risks inclusion strengthens resilience.

Inclusive Design = Secure Design
Systems that adapt to human difference are more trusted, adoptable, and resilient.

error in practice (part a)

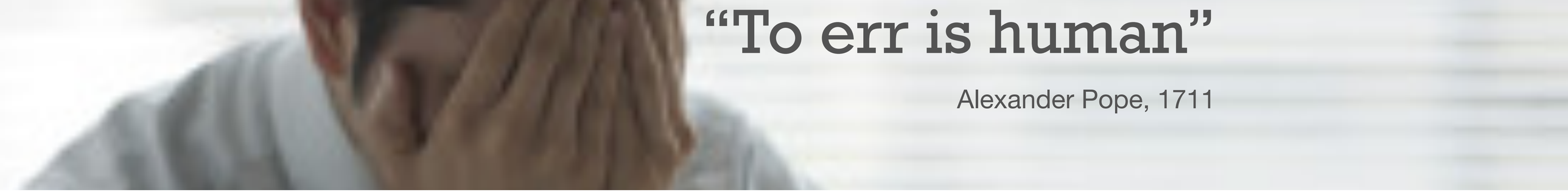
What do we mean by error?

Error is simply a **failure** to adhere to, or **deviation** from, anticipated or expected behaviour.

Error was seen as something “not intended by the actor” but we’ve moved on…

It **can be inadvertent**

It also **can be deliberate**



“To err is human”

Alexander Pope, 1711

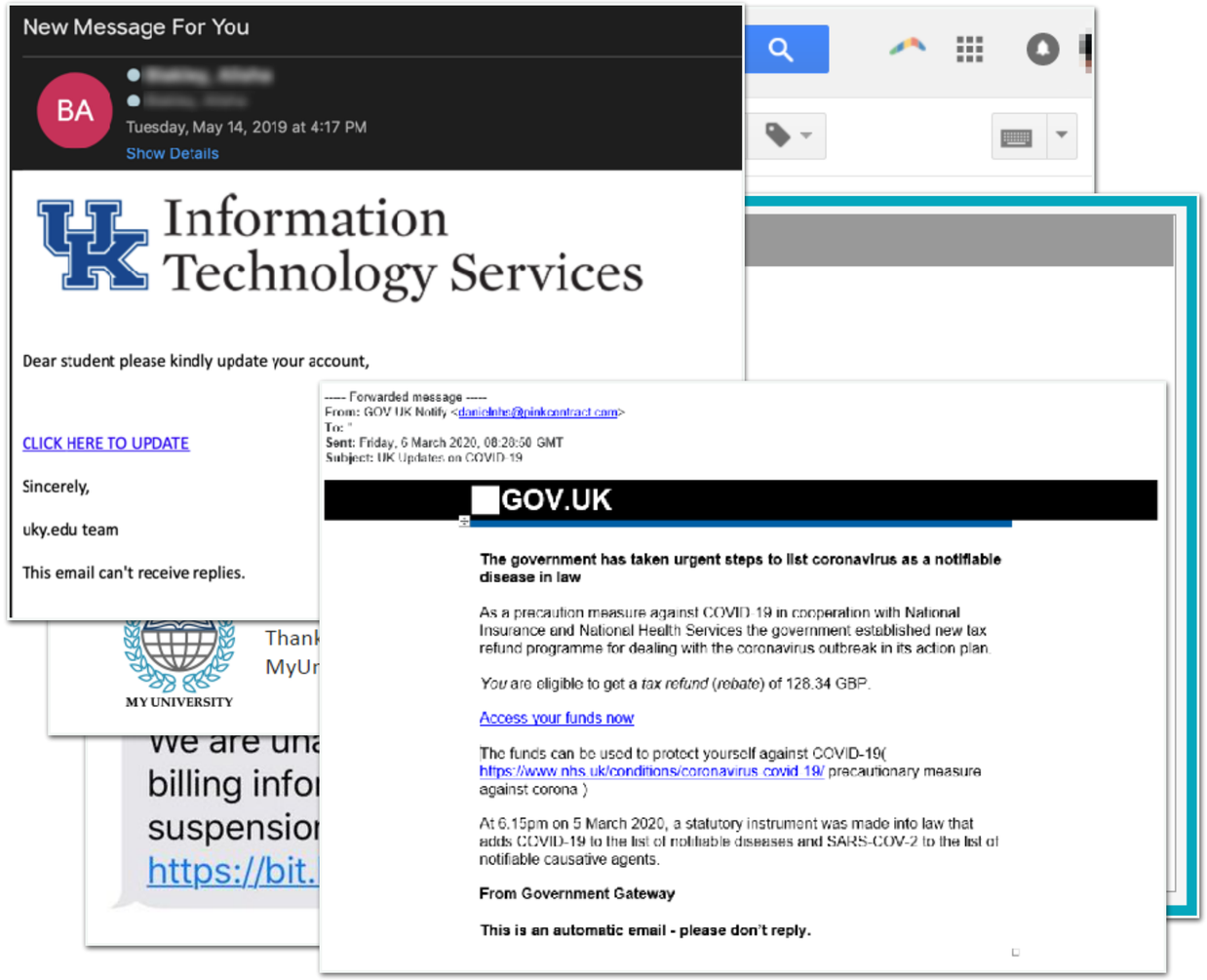
Why do we err?

We’ve already seen that humans are limited in capacity or sometimes unmotivated, easily distracted.

And in these states we end up taking little shortcuts.

In cognitive terms, we revert to System 1 (fast) thinking where we rely on “instinct” - just the wrong instinct. It’s why, when under pressure (pretexts), phishing scams work so well.

[note: we cover Kahneman’s System 1&2 in biases]
[note: Matt looks at phishing in Social Engineering]



The Two Primary Classes of Error

Active Failure (aka Human Error)
These are the errors, [Reason calls them “unsafe acts”], people make inadvertently or deliberately. Active failure tends to have a short-lived but direct system impact.

Latent Failure (aka Design Error)
These are the “resident pathogens” within a system. They are baked in by those people and organisations building the system. They can all but force Active Failure, and may lay dormant for many years. BUT they can be identified and designed out before things turn bad.

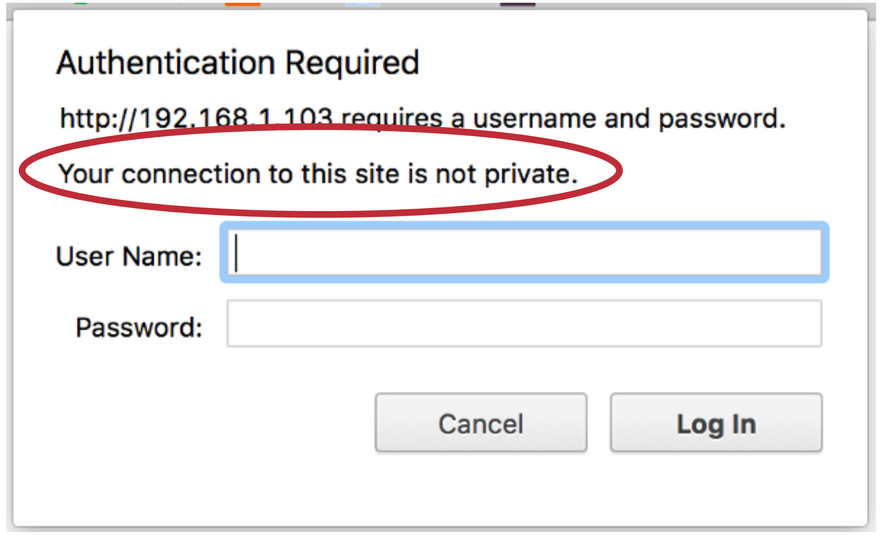
Useful Stuff

Reason, J. 1990
Human Error

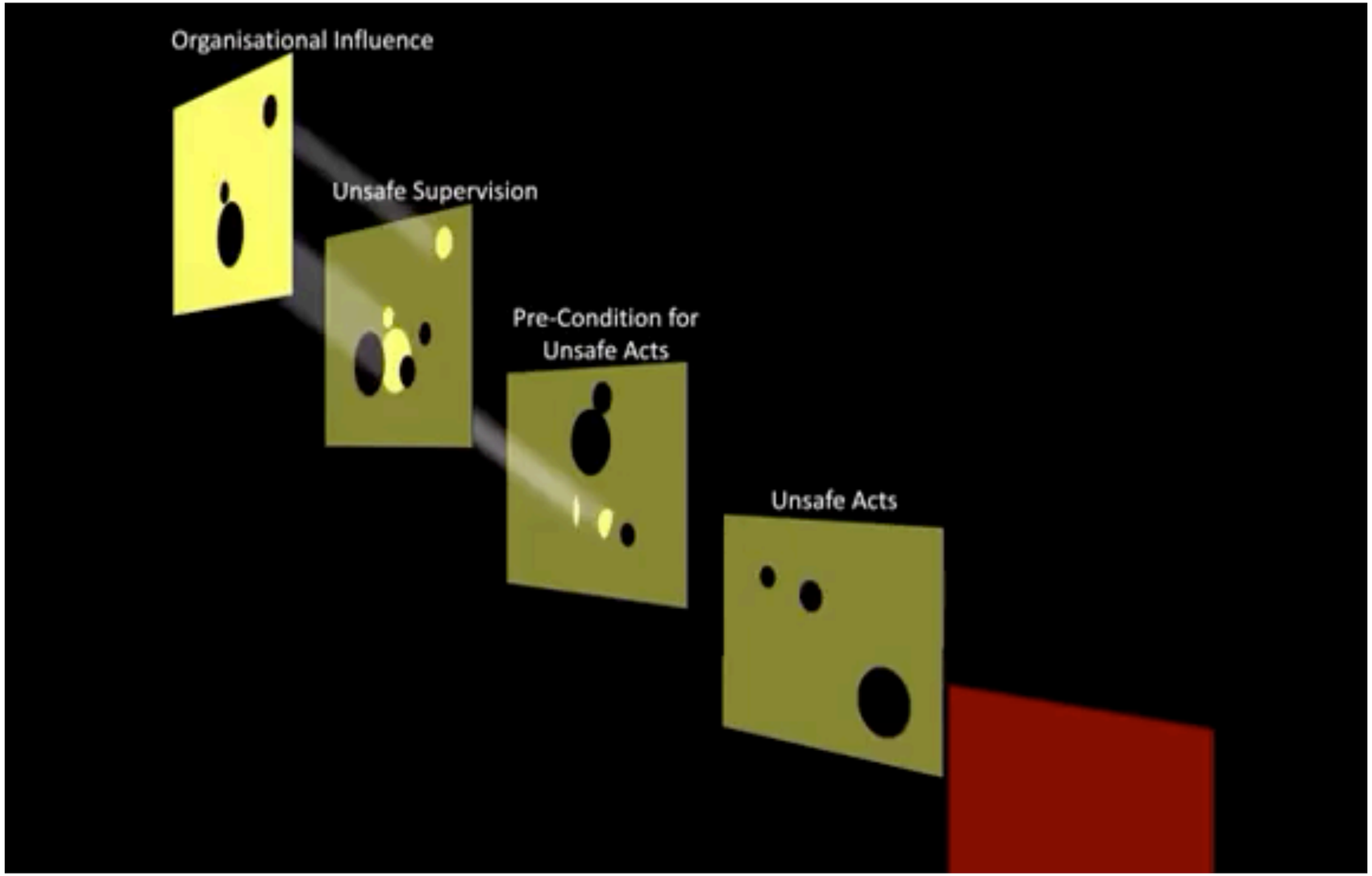
Reason, J. 2000
Human error: models and management
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/

Blythe, J, Koppel, R & Smith, S
2013 Circumvention of Security: Good Users do Bad Things
https://ieeexplore.ieee.org/document/6630017

Latent Failures



Cheesy, Swiss Cheesy

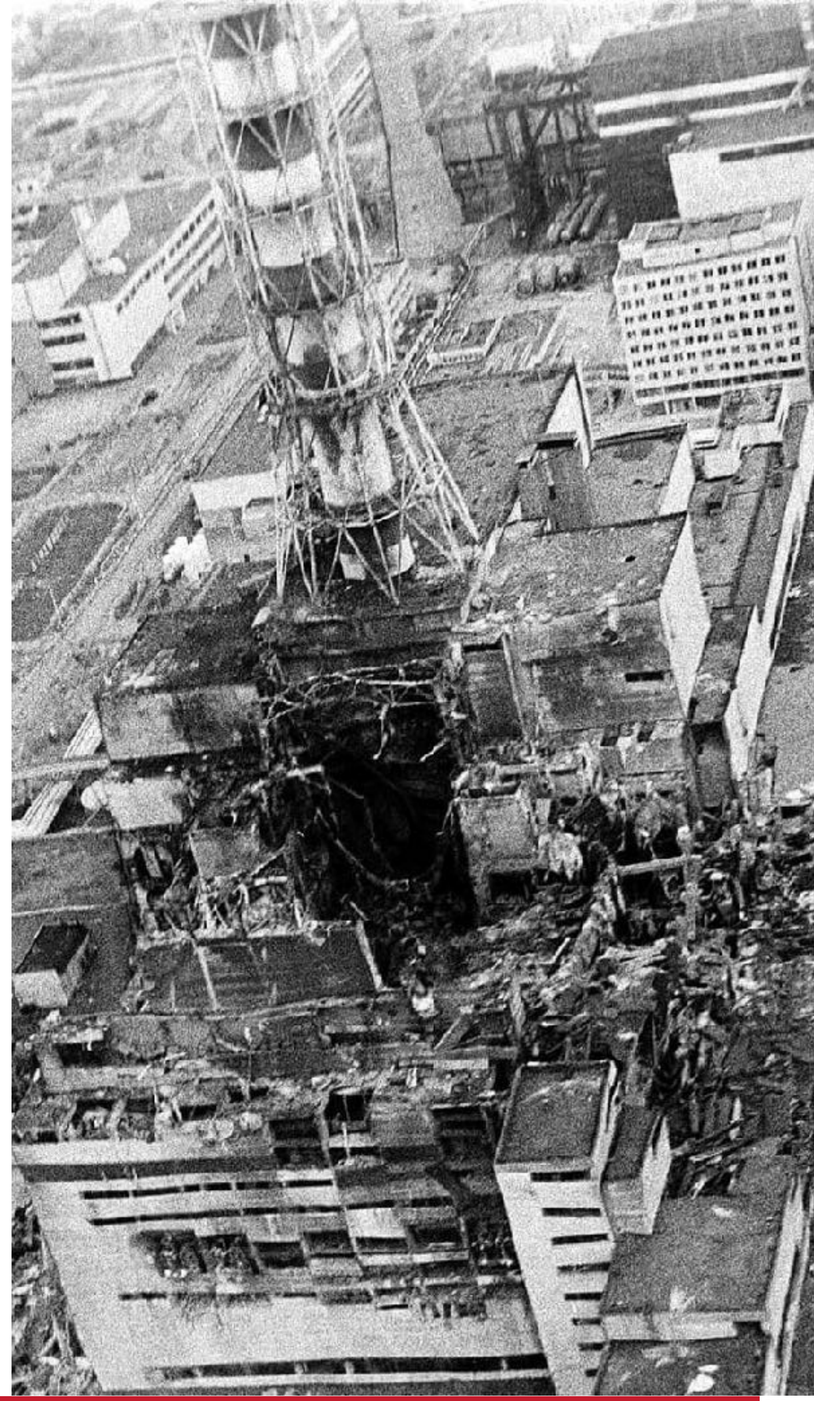


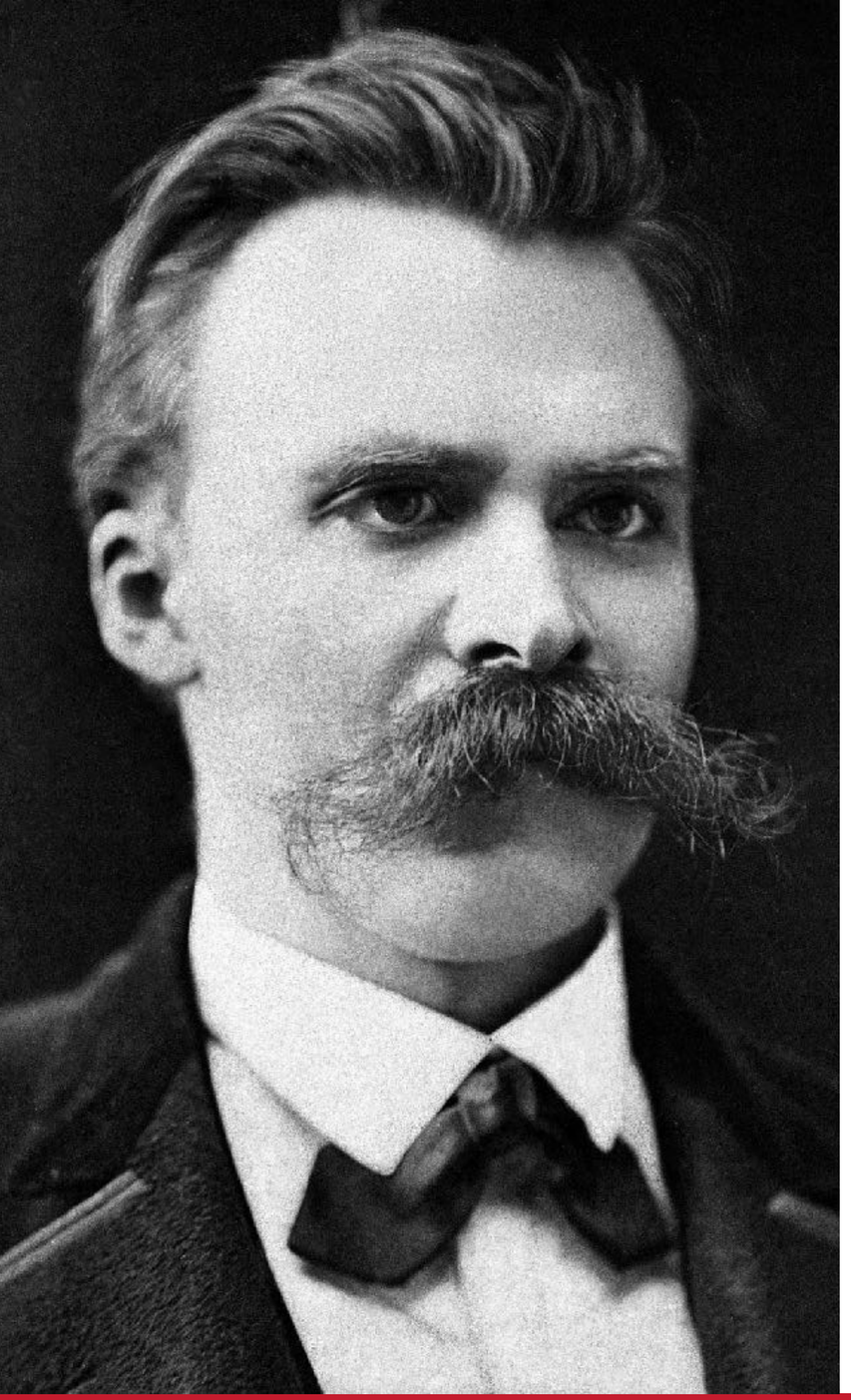
Alignment.. Bad Consequences

Active Failure (aka Human Error)
With the meltdown of reactor no.4, the Chernobyl disaster of 1986 was quite understandably blamed on the operators deliberately violating procedure and manually overriding safety systems in a vain attempt to recover from (yet another) failed test.

Latent Failure
It wasn't until Valery Legasov's own personal audio tapes of events were leaked to the press on his death in 1988 that it was clear the RBMK-1000 reactors not only had a critical design flaw but that i) that flaw had been known to senior party officials, and ii) it hadn't been communicated to operators or operating guidance updated.

The result was all but inevitable given the latent design flaws once the human error occurred.





So if error is “normal” why do we still blame?

“…the need to find a cause, or person/party, responsible is somewhat fundamental to human nature as to not do so implies a loss of control and is distressing.” Nietzsche 1889

Reason’s Person Approach

- Focusses on **errors of the individual**
  “the pilot was to blame for not paying attention”
  “the nurse forgot to administer…”
- Simple, easy and overly focussed on looking for the **root cause** being in these proximal unsafe (insecure) acts.
- Often with reluctance to look further.
- Tends towards solutions to **remove human error.**
- Defers to **blame** and **punishment** as deterrents.

System Approach for Reasoning about Error

"The basic premise in the system approach is that **humans** are fallible and errors are to be expected, even in the best organisations. Errors are seen as consequences rather than causes, having their origins not so much in the perversity of **human nature** as in "upstream" systemic factors." J Reason - **2000**

- Focusses on the conditions under which those individuals work.
- Views error as a **consequence of systemic failure.**
- Looks to contributing or facilitating factors.
- Tries to **build defences** to mitigate effects.
- Countermeasures based on the assumption that though we **cannot change the human condition.**
- When an adverse event occurs, the important issue is not who blundered, but **how and why the defences failed.**

The thing to understand even with a systems approach is that a deliberate and malicious active failure is still blameworthy.

But should this be so, even when latent failure makes the active or outcome inevitable?

University of Bristol Student Agreeme

Definitions

We/Us/Our means the University of Bristol.

You/Your means a registered student of the University of Bristol or someone formally offered a place at the University.

Programme means your course of study or research.

1. Introduction

This Agreement forms the basis of the relationship between you and the Uni you accept an offer of a place for your Programme. Through annual registrati

- comply with all Uni

Penalties for misuse

Minor breaches of policy will be dealt with by IT Services. Heads of Department

- Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of the University.

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

University of Bristol
Information Security Policy

Title: **Acceptable Use**
Reference: **ISP-09**
Status: **Approved**
Version: **1.1**
Date: **October 2016**
Review: **February 2019**

Contents

- Introduction

ation

networks

(Software Engineering) Problem Space

Security work has often focussed upon technical advancement - the **build a better mousetrap** approach. This aligns with the person approach for reasoning about error.

As we've seen humans - through error or mistake (intentional or otherwise) - are often seen as at fault or to blame for security problems with a **culture-of-blame** leading "to a misconception that better security comes from better systems." i.e., it's a self fulfilling prophecy.

"The more effort placed into better smarter technology the more likely it is that, in the event of failure, the human is seen as in error and therefore further effort needing to be put into further technological improvement."

But safety research demonstrates that technical improvement can sometimes cater for human (cognitive) capacity there is a point at which "**automation... simply shifts the error**" – normally to the designer / developer." And this is where we have to be a little self aware that we too are human.