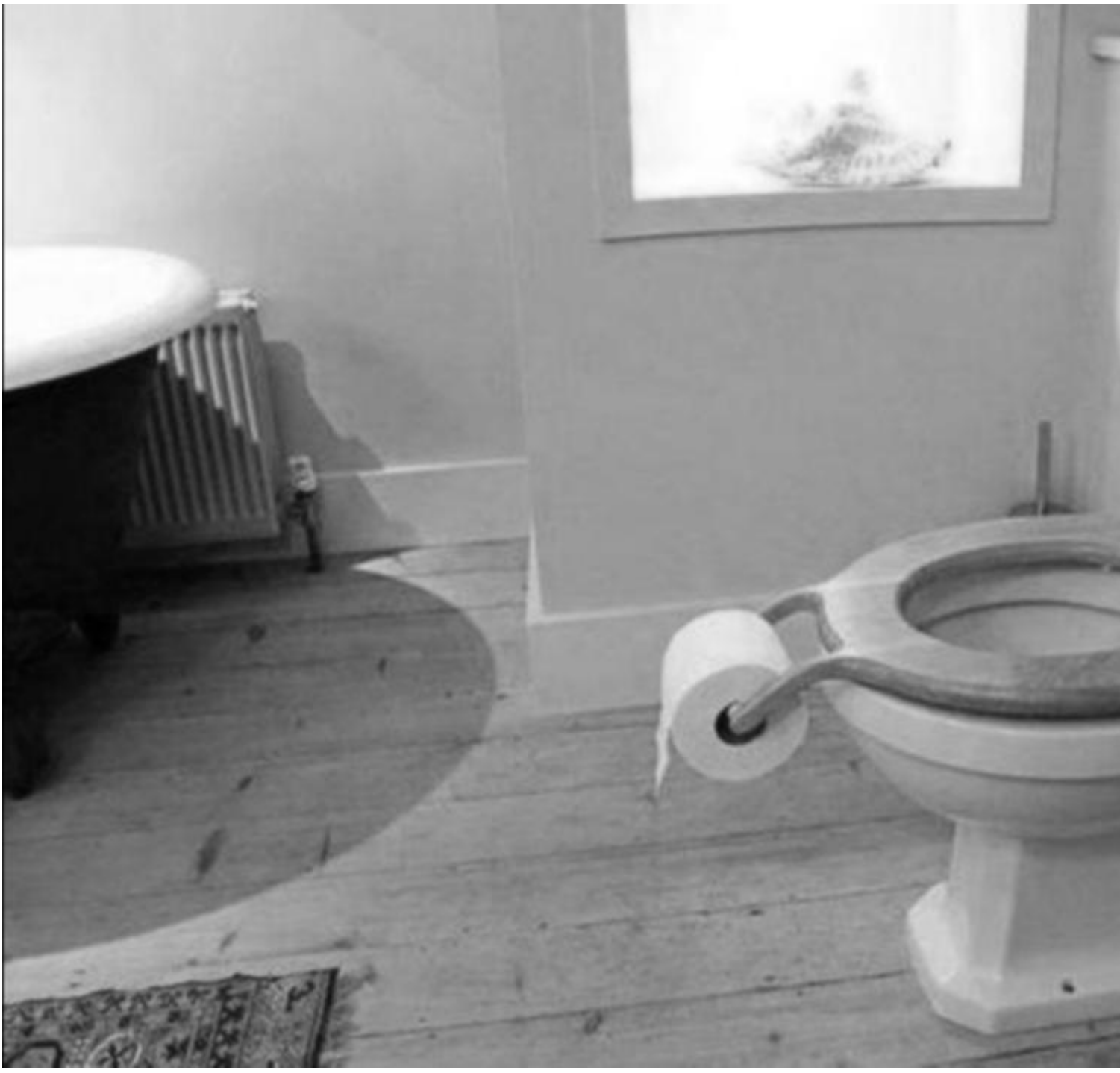
ObSec

TEFLONRABBIT ARTICLE No.173

Unique Identifier:002ded56-46d9-4964-a73e-87840c09df25



Complacency through idiocracy

Sunday, January 31, 2021 - 19:59

PDF Version
Aroma

Image not found or type unknown

50
Rumness
Image not found or type unknown

60
Subscription Only
Off

There's a highly questionable practise witnessed in development known as 'security through obscurity'. It involves using ridiculously conceived and unorthodox methods in order to achieve some form of protection against known vulnerabilities.

SDLC *Commercial* *Technical* *Bovine Excretia* *Obscurity* *Value* *Revenue* *Bad practice* *Communication*

Frequently the chosen methods have not been selected according to any type of 'best practice' and instead have more to do with alleged cost saving, intransigence, insufficient development resource or lack of familiarity with conventional methods.

Generally the support for such methods comes from somewhere closer to the commercial side rather than the technical side. This is understandably due to the commonly held belief among commercial depts that shortcuts and workarounds can be considered acceptable as long as the billing is not impacted.

For any technical staff, the result is often quite alienating. Furthermore it serves to widen the philosophical chasm between commercial and technical teams.

During a meeting between a commercial team, a project manager and a head of development; the issue of recycling existing projects was raised. This technique has caused numerous issues with product usability since the days of Charles Babbage. The technical team was quite committed to the prevention of unmet expectations arising from minimal communication.

"At some point, we need to stop hacking and start building. What we've been doing is developing shanty towns. What the average punter wants is a semi detached or mid terraced house with conventional bedrooms upstairs and a bit of a garden out the back. Delivering yet another corrugated iron shack with no running water can only be considered as kicking the can down the road."

The head of development was attempting to strike the right balance between justified alarmism and the unavoidable requirement for 'people first' attitudes when it comes to delivering bad news.

Unfortunately, this consideration to the emotional well-being of the commercial team was blatantly capitalised on and the project manager responded with ...

"But we've built a BRAND NEW shanty town, so ....."

Really the best thing the head of development could have done at this point would be to kick the table over and leave the meeting. However, such responses are generally considered to be unreasonable and as such they merely sighed and rolled their eyes.

"Did you really just say 'a brand new shanty town'?"

"Well . .. YES! - what's wrong with that. We've delivered it before and made money so why don't we just do the same thing again? - and maybe roll it out to a whole load of other customers as well"

"Because (as mentioned) humans don't actually want to live in tin huts. They're too hot in the summer, too cold in the winter and basically many years of construction sales have established the fact that it's a mistake to sell shacks as homes."

"But ... er .... ummm .." (looks at floor)

While this scenario specifically highlights the disadvantages of short term thinking in regards to SDLC, it serves as a suitable metaphor in the deployment of *'security through obscurity'*. Ignoring convention and best practice in favour of a less pragmatic approach constitutes a similarly ill conceived methodology. Any cost savings will be negated as a result of increases in development and support hours. Facilitating weak methodology can lead to multiple points of failure. Operating any commercial enterprise without best practice policies can only be considered in the short term.

Essentially this communication disaster stems from a defence of the choices previously made, something along the lines of;

"Oh well this is the situation we've created, so everyone will just have to adapt and overcome"

Again, the appropriate response involves kicking tables over and storming out of the meeting.
Expecting those responsible for delivering a product to repeatedly jump through pointless hoops but still meet deadlines and budgets is just unrealistic. It represents a far more strategic approach to follow convention and best practise policies that have been developed and ratified by the product delivery community.