FLUSHING AWAY PRECONCEPTIONS OF RISK

Thom Langford
@thomlangford

October 2015

DISCLAIMER

The opinions expressed in this presentation are my own and do not necessarily represent those of my employer

@thomlangford

- our interpretation of risk
- our measurement of risk
- our effective treatment of risk


@thomlangford

@thomlangford

@thomlangford


@thomlangford

@thomlangford

@thomlangford

49 sq/in

@thomlangford

1,676 sq/in

3,295 sq/in

@thomlangford

20,961 sq/in

@thomlangford

25,127 µl/s

@thomlangford

@thomlangford

"*perceived*" risk

"*hygiene*" risk

"*actual*" risk

THE MEASUREMENT OF RISK

The Malik Risk Model Ver 1.0		Impact			
		Won't Hurt	Is that the best you got?	Ouch!	Holy Crap!
Likelihood	Ain't Happening	"a swift half"	"it's your round"	"easy Tiger…"	"hold my drink Steve"
	Possibly	"it's your round"	"easy Tiger…"	"hold my drink Steve"	"Get off him Dave, he ain't worth it"
	It's On	"easy Tiger…"	"hold my drink Steve"	"Get off him Dave, he ain't worth it"	"cab to A&E please"
	Holy Crap!	"hold my drink Steve"	"Get off him Dave, he ain't worth it"	"cab to A&E please"	"Ambulance please"

Malik, Javvad (2014-05-12). The CISSP companion handbook: A collection of tales, experiences and straight up fabrications fitted into the 10 CISSP domains of information security (Kindle Locations 918-923). . Kindle Edition.

@thomlangford

The Langford/ Malik Risk Model ver 1.0	Likelihood of threat	Ain't Happening			It's On!			Holy Crap!		
	Ease of Exploitation	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk
Asset Value	Arm	"It's your round"	"have a word, mate"	"easy Tiger…"	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"
	Leg	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"
	Chest	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"
	Face	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"
	Testicles	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"	"cab to A&E please"	"Ambulance please"	"Mortuary please"

@thomlangford

The Langford/ Malik Risk Model ver 1.0	Likelihood of threat	Ain't Happening			It's On!			Holy Crap!		
	Ease of Exploitation	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk
Asset Value	Arm	"It's your round"	"have a word, mate"	"easy Tiger…"	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"
	Leg	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"
	Chest	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"
	Face	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"
	Testicles	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"	"cab to A&E please"	"Ambulance please"	"Mortuary please"

@thomlangford

18-24 YEAR OLD (SINGLE & UP FOR IT)

The Langford/ Malik Risk Model ver 1.0	Likelihood of threat	Ain't Happening			It's On!			Holy Crap!		
	Ease of Exploitation	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk	I'm a Ninja	I'm a drunk Ninja	I'm drunk
Asset Value	Arm	"It's your round"	"have a word, mate"	"easy Tiger…"	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"
	Leg	"have a word, mate"	"easy Tiger…"	"cheeky slap"	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"
	Chest	"easy Tiger…"	"cheeky slap"	"get off him Dave"	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"
	Face	"cheeky slap"	"get off him Dave"	"Let's 'ave it then"	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"
	Testicles	"get off him Dave"	"Let's 'ave it then"	"cab to A&E please"	"Let's 'ave it then"	"cab to A&E please"	"Ambulance please"	"cab to A&E please"	"Ambulance please"	"Mortuary please"

@thomlangford

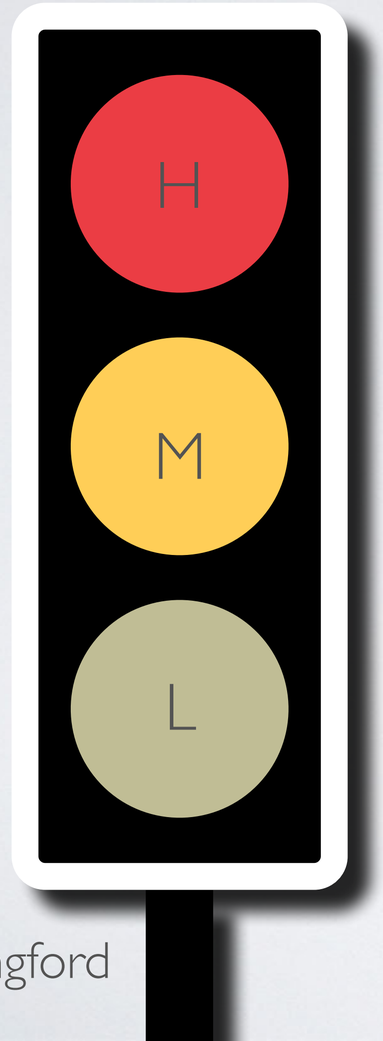
40 YEAR OLD (MARRIED WITH KIDS)

ISO 27005 Risk Model	Likelihood of threat	Low			Medium			High		
	Ease of Exploitation	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

@thomlangford

IN PRACTISE

WHAT'S WRONG WITH ORDINALS?



And nobody uses "red" because it means failure

Therefore the risk world becomes "amber"

Nobody uses "green" because it means no more budget

Nassim Nicholas Taleb,
''The Black swan''

@thomlangford

@thomlangford

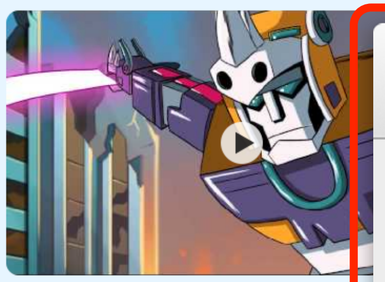
THE TREATMENT OF RISK

@thomlangford

@thomlangford


@thomlangford

@mduren all together, is it like one inch? Still arguing over the head? youtube.com/watch?v=EMgsAD…



Peopple these days just don't respect embargoes!

8 hours

naked selfies, had them hacked, but nobody seems to want to share them (or admit to having them).

HostUnknownTV @HostU… 32d

Security & Privacy

Show All

General | FileVault | Firewall | Privacy

FileVault secures the data on your disk by encrypting its contents automatically.

Turn Off FileVault…

FileVault is turned on for the disk “Macintosh HD”.

A recovery key has been set.

Click the lock to make changes.

Advanced…

?

sir jester @sirjester
@EdwardPrevost @J4vv4D @ThomLangford @jack_da… @mduren The collective po… our beards is underrated! pic.twitter.com/ECbw0uuCWB

Edward Prevost @Edward…
@sirjester @J4vv4D @ThomLangford heh You'll be fashionable when yo… sport an epic beard. (cc @jack_daniel @mduren)

sir jester @sirjester
@J4vv4D @ThomLangford I'll concede they're better than the sexist swag you produce! :)

TheAnalogies Project @TheA… 4h

think he wants to move (in fact I wouldn't let him!)

6 hours

HostUnknownTV @HostUnkn… 43d
To all of our Indian fans, “AP BINDAAS HO!” #HostUnknownLovesIndia

Debasish @thisisdebasish 19d
@sirjester @chrisriceuk @HostUnknownTV Enjoy the evening brothers! Cheers!

sir jester @sirjester 19d
@thisisdebasish @chrisriceuk We're already planning the next @HostUnknownTV hit (not in pwnie terms but as an ear-worm) ;)

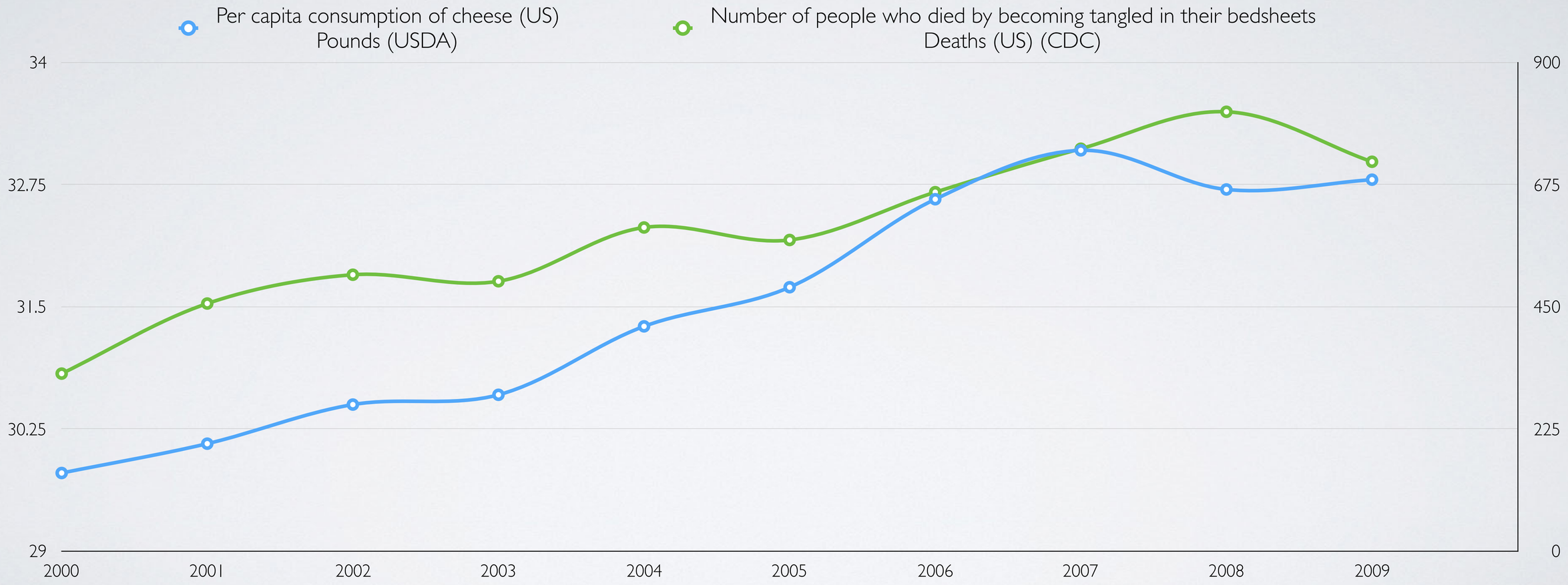
Info Security Buzz @Info_Sec… 22d
.@metasploit, Apple, and #Snowden: The Legends of #Infosec informationsecuritybuzz.com/metasploit-app… Andrew Agnes, Thom Langford & Javvad Malik, @HostUnknownTV

Info Security Buzz @Info_Sec… 28d
.@metasploit, Apple, and #Snowden: The Legends of #Infosec informationsecuritybuzz.com/metasploit-app… Andrew Agnes, Thom Langford & Javvad Malik, @HostUnknownTV

Info Security Buzz @Info_Sec… 29d
.@metasploit, Apple, and #Snowden: The Legends of #Infosec informationsecuritybuzz.com/metasploit-app… Andrew Agnes, Thom Langford & Javvad Malik, @HostUnknownTV

sir jester @sirjester 32d
@HostUnknownTV @RANTConference Um, I have some bad news about that champagne...

CAUSATION VS CORRELATION



Source: Spurious Correlation, www.tylervigen.com

FLEXIBLE RISK RESPONSE

TAKEAWAY #1

- Recognise and understand the difference between "hygiene" risks and "actual" risks

TAKEAWAY #2

- Spot patterns in your risks over time.
  What has become a commodity?
  What were the black swans?

TAKEAWAY #3

- A risk hasn't been mitigated just because it hasn't happened; don't suffer a placebo effect.

thom@thomlangford.com

@thomlangford

uk.linkedin.com/in/thomlangford