



WHAT

UFO'S, DIRTY DANCING & EXPLODING HELICOPTERS

UNDERSTANDING RISK MANAGEMENT HOLLYWOOD STYLE

WHEN

16TH MAY 2013

WHERE

ISSA-UK BRISTOL



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



What are we talking about?

- * Ten risk management points of view
- * Ten famous movie quotes, and four bonus questions
- * There are prizes!
- * One prize per person, per question
- * Only one prize per person, offer valid only on the night of ISSA-UK, 16th May 2013, family and friends of Thom Langford are not eligible to enter, no purchase necessary, no cash alternative, the judges decisions are final, no correspondence will be entered into, by participating in tonights ISSA-UK presentation you agree to applaud and cheer heartily at the end and speak well of Mr Langford and his affiliates for at least three generations; local laws may prohibit participation and winners will be responsible for their own personal tax liability to the full cash value of the prize and upon acceptance of said prize will abide by these rules and any conditions.

@thomlangford

#1

“You’re gonna need a bigger boat”



POLICE CHIEF MARTIN BRODY

JAWS

@thomlangford

Don't underestimate your risks

- ✱ Even if you are small, you are still a target ₁
- ✱ Ensure you measure your risks effectively and accurately
- ✱ Don't think "unlikely" events will not happen
- ✱ Be realistic and avoid "wild dog syndrome"
- ✱ Plan for failure, these risks are real and not just reference points

#2

“I’ll be back”



THE TERMINATOR

THE TERMINATOR

@thomlangford

Risks don't go away

- * Even if you have mitigated, avoided, transferred or accepted
- * Risks are always present, just less likely or somewhere else
- * Review them regularly, at least annually
- * What has changed? Likelihood, Ease of Exploitation?
- * Even company's risk appetite can change

#3

**"Badges? We ain't got no
badges. We don't need no badges!
I don't have to show you any
stinkin' badges!"**



“GOLD HAT”

THE TREASURE OF THE SIERRA MADRE

@thomlangford

The CRISC doesn't make you ready

- * Or any other qualification
- * You need experienced as well as eager people
- * They help in the first rounds of an interview only
- * Qualifications demonstrate existing foundation knowledge only
- * They are too often presented as evidence of experience

#4

“Open the pod bay doors HAL”



DR. DAVE BOWMAN

2001: A SPACE ODYSSEY

@thomlangford

You can't just rely on technology

- * Technology, has, does and will fail
- * But so will humans!
- * Complement your technological controls with soft controls
- * All of your staff and people are security advocates
- * Technology helps with automation and the mundane

#5

“I see dead people”



COLE SEAR
THE SIXTH SENSE

@thomlangford

Be careful of professional burnout

- * “Burnout” in infosec professionals is increasingly recognised ₂
- * One study found 70 to 80 hours per week is *normal*
- * Job creep is common, with responsibilities split
- * Perpetual work (more risks, viruses, incidents), no end in sight
- * The economy has made this worse

#6

“My precious”



GOLLUM

LORD OF THE RINGS: THE TWO TOWERS

@thomlangford

Look after your (precious) data

- * Do you know what systems your data resides in?
- * Do you know what country it resides in?
- * Do your people know where it should reside?
- * Do you know how long you have had it for?
- * Do you know what regulatory and legal requirements you have?

#7

“Houston, we have a problem”



JIM LOVELL (JACK SWIGERT)

APOLLO 13

@thomlangford

Risk Management? Incident Management?

- ✱ Both identify / detect
- ✱ Both classify / assess
- ✱ Both apply resources / recover
- ✱ Both control / resolve
- ✱ How closely tied is your incident management to your risk management programme?

#8

“Nobody puts baby in a corner”



JOHNNY CASTLE

DIRTY DANCING

@thomlangford

Manage risks from the top down

- * Your organisational structure will often reflect your success
- * Who do you escalate enterprise risks to?
- * A formal process of escalation must exist for it to be effective
- * The “tone at the top” must be supportive
- * Empowerment to deal with risks must exist at all levels

#9

“No Mr Bond, I expect you to die”



GOLDFINGER

AURIC GOLDFINGER

GOLDFINGER

@thomlangford

Don't reveal your internal documents

- * Internal documents appear outside, everywhere, all the time! ₃
- * At best it is embarrassing
- * At worst it results in competitive loss, lawsuits, financial loss
- * Categorise ALL documentation, educate, use technology
- * Get your basics covered, build on these foundations

#10

**“They’ve done studies, you know.
Sixty percent of the time, it works
every time.”**



RON BURGANDY

ANCHORMAN

@thomlangford

Lies, damn lies and statistics

- ✱ *“Reduce phishing click throughs by 75%!”* ₄
- ✱ *“...successfully trained over 7000 employees”* ₅ (Fox Entertainment)
- ✱ Statistics are often used to sell and also to scare you to buy
- ✱ Use statistics carefully and responsibly
- ✱ If you can’t “reverse” the statistic, don’t use it or believe it

Bonus Round #1

Risky Business



Bonus Round #2

Maximum Risk



Bonus Round #3

Risk



@thomlangford

Bonus Round #4

Paul Blart Mall Cop



@thomlangford

Questions

Thank You



@ThomLangford



<http://uk.linkedin.com/in/thomlangford>



thom@thomlangford.com

Copyright & Credits

✱ “Jaws” Universal Studios

✱ “The Treasure of the Sierra Madre” Warner Brothers

✱ “2001: A Space Odyssey” MGM/Warner Brothers

✱ “Goldfinger” United Artists

✱ “Anchorman: The Legend of Ron Burgandy” Dreamworks Pictures

✱ “Dirty Dancing” United Artists

✱ “Apollo 13” Universal Pictures

✱ “Terminator” Orion Pictures

✱ “Risky Business” Warner Brothers

✱ “Paul Blart Mall Cop” Columbia Pictures

✱ “Risk” *Unknown*

✱ “The Lord of the Rings: The Two Towers” new Line Cinema

✱ “The Sixth Sense” Hollywood Pictures

✱ “Maximum Risk” Sony/Columbia

1. [krebsonsecurity](#)

2. [Security Burnout & The Register](#)

3. Google [“leak of internal documents”](#)

4. [KnowBe4](#) Internet Security Awareness Training

5. [TerraNova](#) Security Awareness

@thomlangford