Twitter : @curphey
RSS : www.curphey.com
Email : mark@curphey.com

SWEDEN

BlogWorthy.com
FEYENOORD
F
ROTTERDAM

ND
THE REST

10
9
10
9

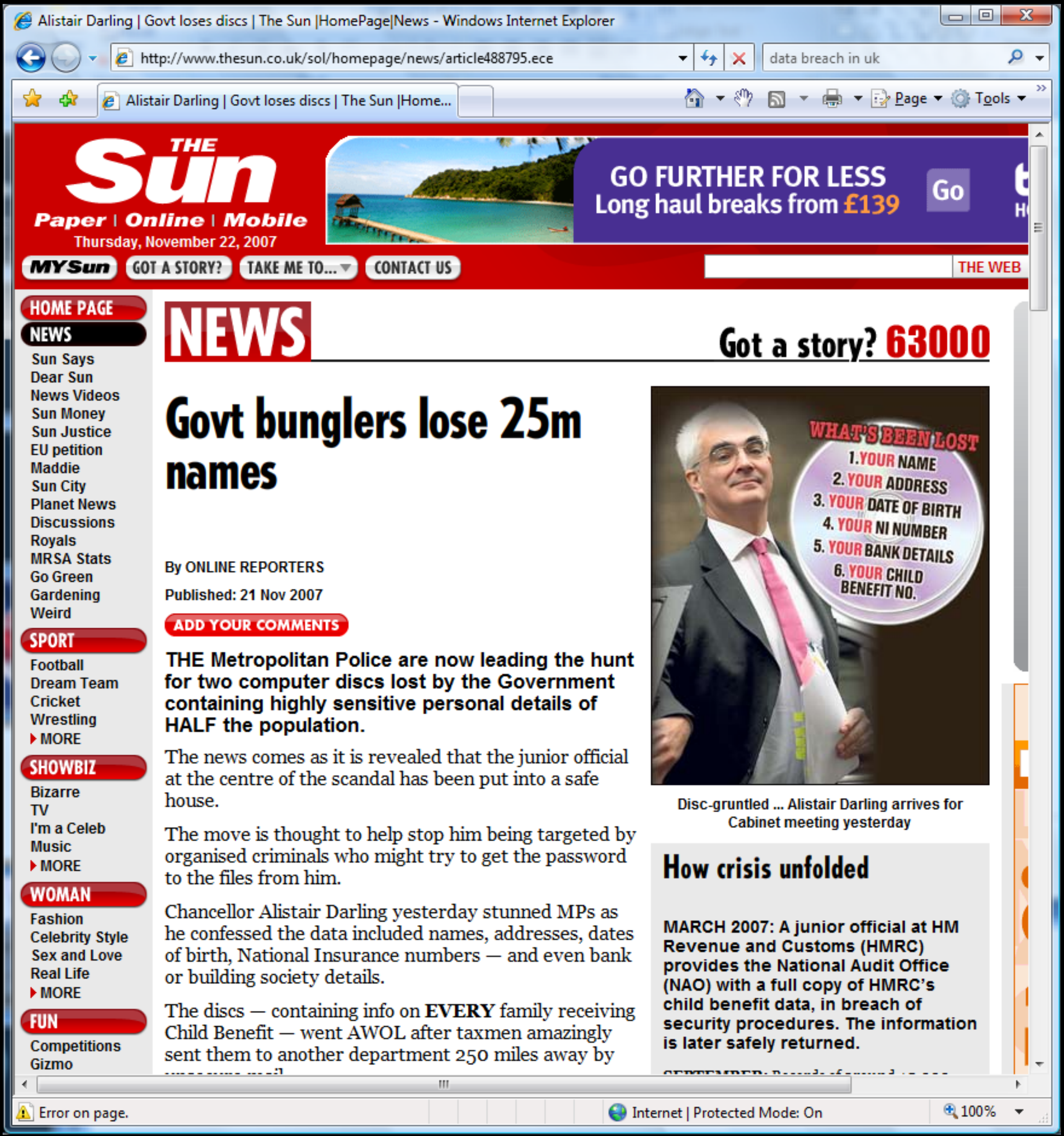
US

What a shame…..”cry-baby”

10

adidas
adidas
ARGENTINA
10

ORDEM E PROGRESSO
BRAZIL
ZWANI.COM



Alistair Darling | Govt loses discs | The Sun |HomePage|News - Windows Internet Explorer
http://www.thesun.co.uk/sol/homepage/news/article488795.ece
data breach in uk
Alistair Darling | Govt loses discs | The Sun |Home...
Page
Tools

THE Sun
Paper | Online | Mobile
Thursday, November 22, 2007

MYSun
GOT A STORY?
TAKE ME TO...
CONTACT US
THE WEB

NEWS

Got a story? 63000

Govt bunglers lose 25m names

By ONLINE REPORTERS

Published: 21 Nov 2007

ADD YOUR COMMENTS

THE Metropolitan Police are now leading the hunt for two computer discs lost by the Government containing highly sensitive personal details of HALF the population.

The news comes as it is revealed that the junior official at the centre of the scandal has been put into a safe house.

The move is thought to help stop him being targeted by organised criminals who might try to get the password to the files from him.

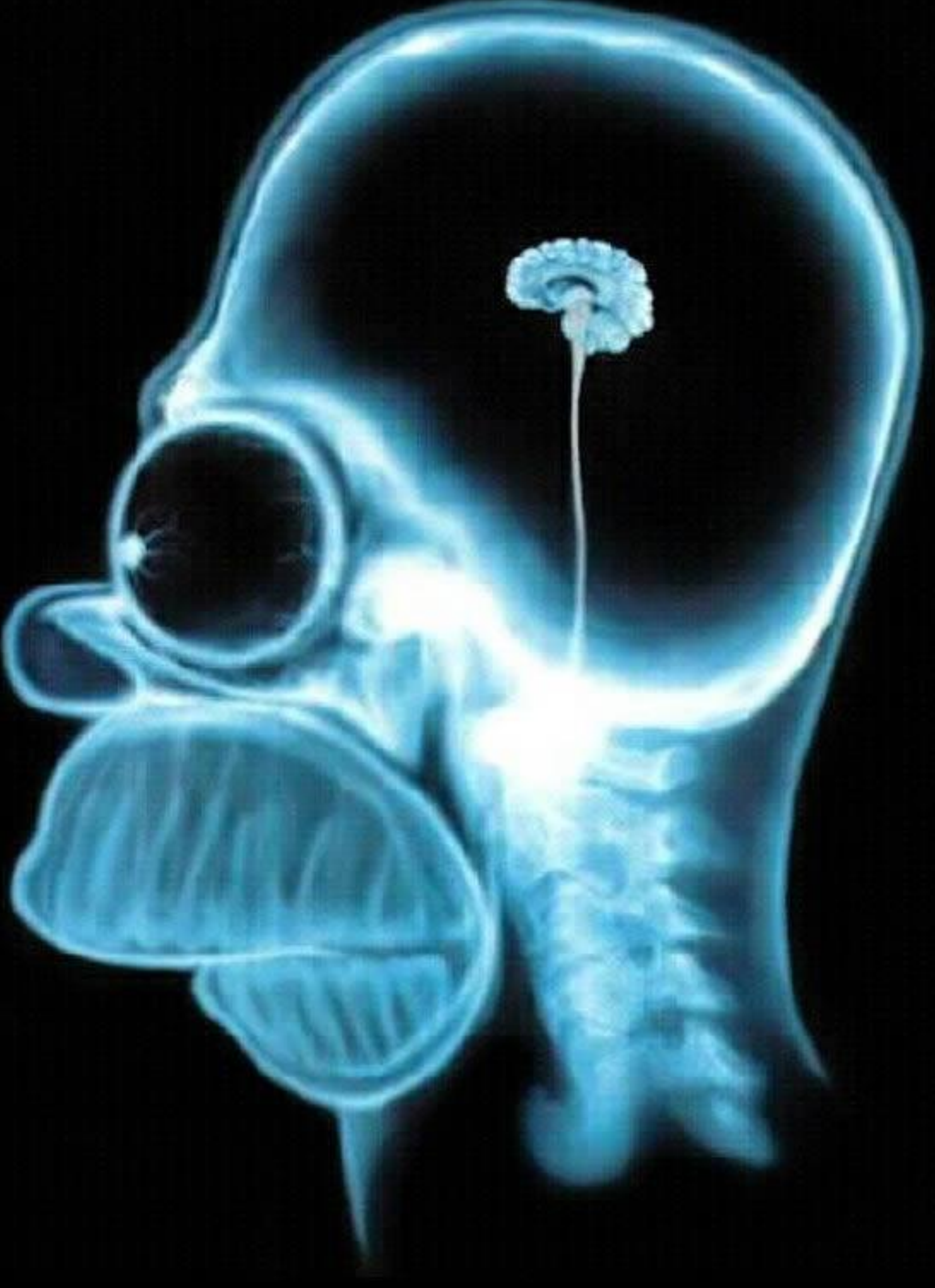
Chancellor Alistair Darling yesterday stunned MPs as he confessed the data included names, addresses, dates of birth, National Insurance numbers — and even bank or building society details.

The discs — containing info on **EVERY** family receiving Child Benefit — went AWOL after taxmen amazingly sent them to another department 250 miles away by

Disc-gruntled ... Alistair Darling arrives for Cabinet meeting yesterday

How crisis unfolded

MARCH 2007: A junior official at HM Revenue and Customs (HMRC) provides the National Audit Office (NAO) with a full copy of HMRC's child benefit data, in breach of security procedures. The information is later safely returned.



VOLUME
TONE
TONE

.com

charles SCHWA
N SDAQ ied S
NASDAQ

About The Open Web Application Security Project

Guide Table of Contents

Contents [hide]

Overview

[edit]

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security includes

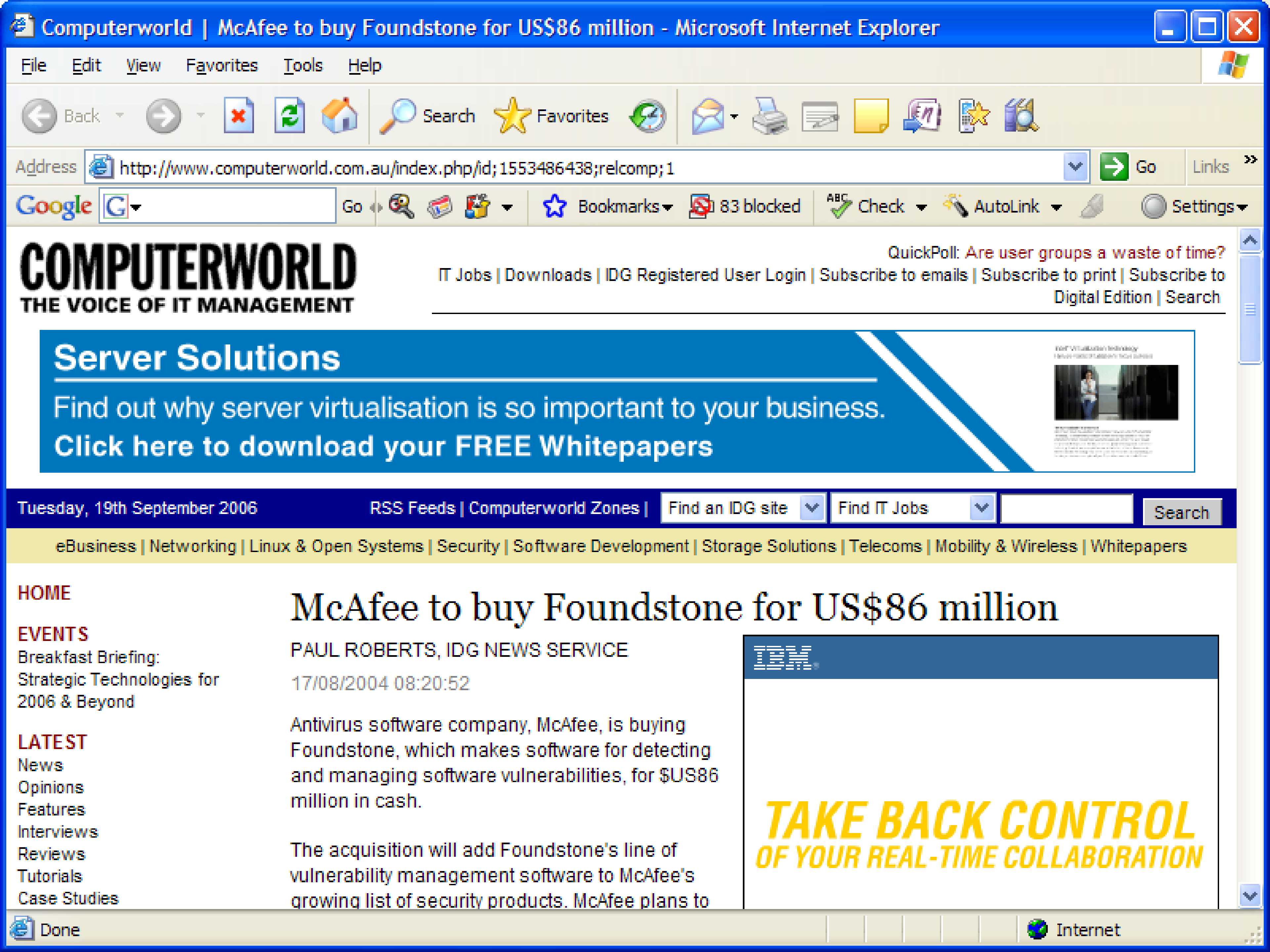
.com

FOUNDSTONE

KNOW VULNERABILITIES

Managed Security Services
Professional Services
Education

www.foundstone.com


Computerworld | McAfee to buy Foundstone for US$86 million - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.computerworld.com.au/index.php/id;1553486438;relcomp;1
Go
Links
Google
Go
Bookmarks
83 blocked
Check
AutoLink
Settings
Done
Internet

COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

QuickPoll: Are user groups a waste of time?

IT Jobs | Downloads | IDG Registered User Login | Subscribe to emails | Subscribe to print | Subscribe to Digital Edition | Search

Tuesday, 19th September 2006 RSS Feeds | Computerworld Zones | Find an IDG site Find IT Jobs Search

eBusiness | Networking | Linux & Open Systems | Security | Software Development | Storage Solutions | Telecoms | Mobility & Wireless | Whitepapers

HOME

EVENTS
Breakfast Briefing: Strategic Technologies for 2006 & Beyond

LATEST
News
Opinions
Features
Interviews
Reviews
Tutorials
Case Studies

McAfee to buy Foundstone for US$86 million

PAUL ROBERTS, IDG NEWS SERVICE

17/08/2004 08:20:52

Antivirus software company, McAfee, is buying Foundstone, which makes software for detecting and managing software vulnerabilities, for $US86 million in cash.

The acquisition will add Foundstone's line of vulnerability management software to McAfee's growing list of security products. McAfee plans to

Microsoft®

Vision or Delusion? You Decide!

(either way hopefully it will be fun)

People solve complex problems

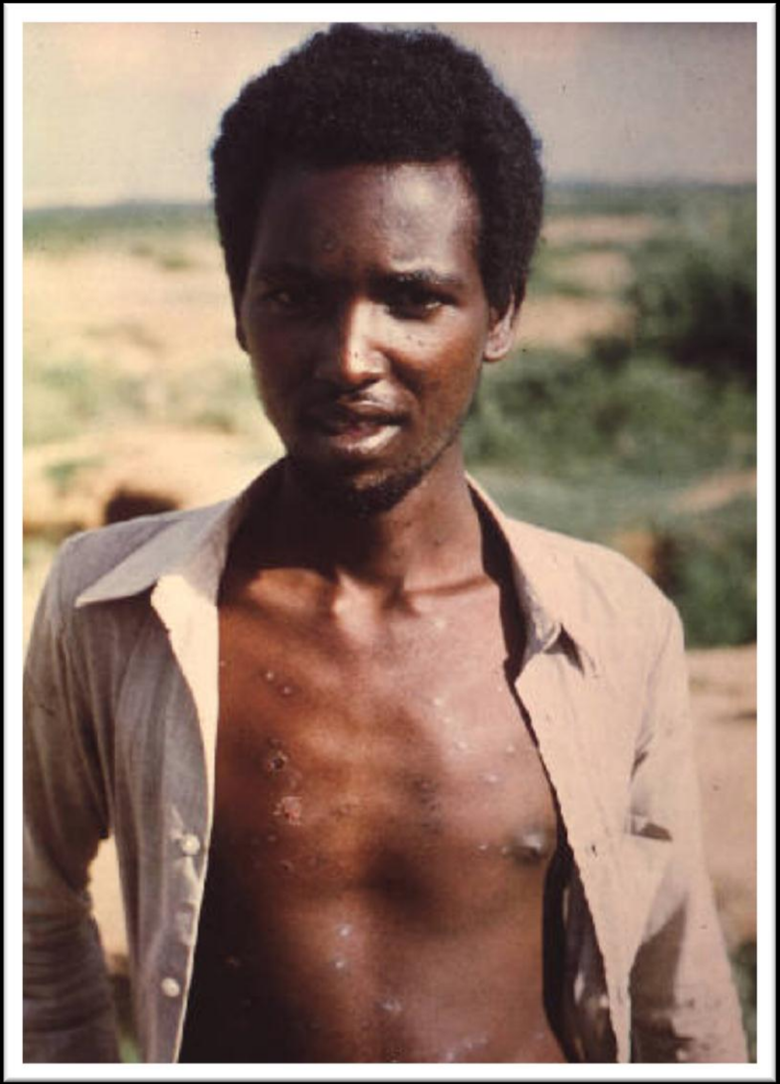


Photo: Wikimedia

- Smallpox
- Deadliest disease in history
- 1900-1979
  - 500 million victims died
  - 15 million per year in 60s
  - ½ of all blindness in Asia

People solve complex problems

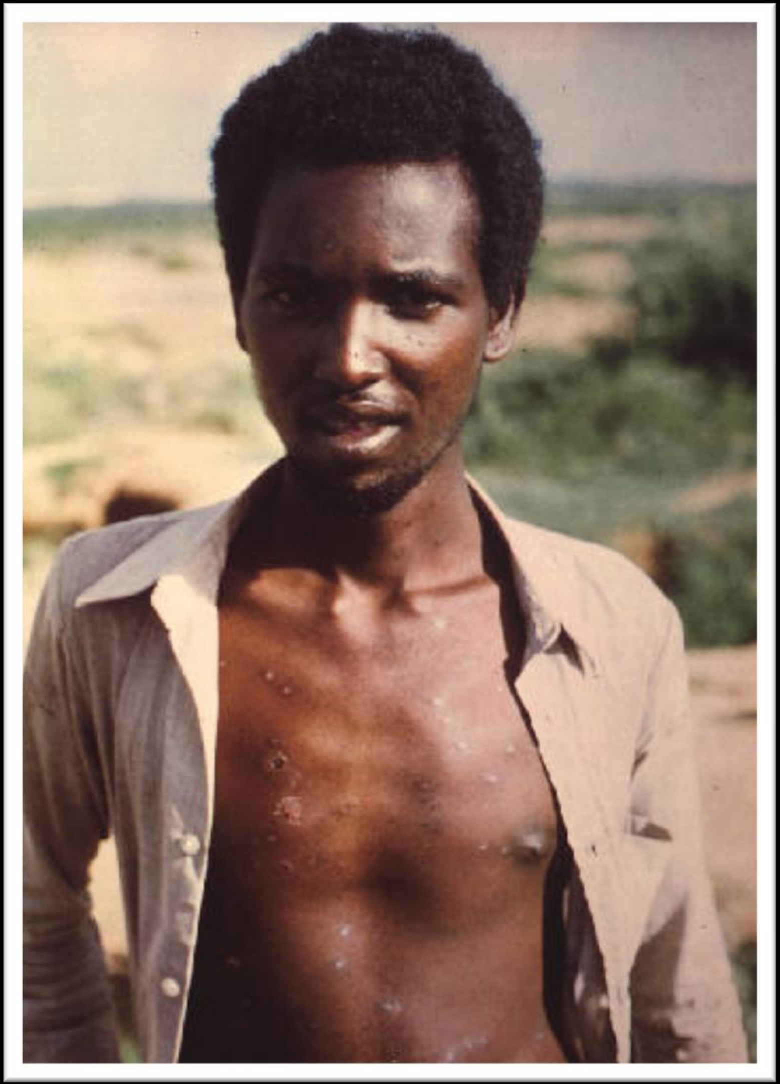
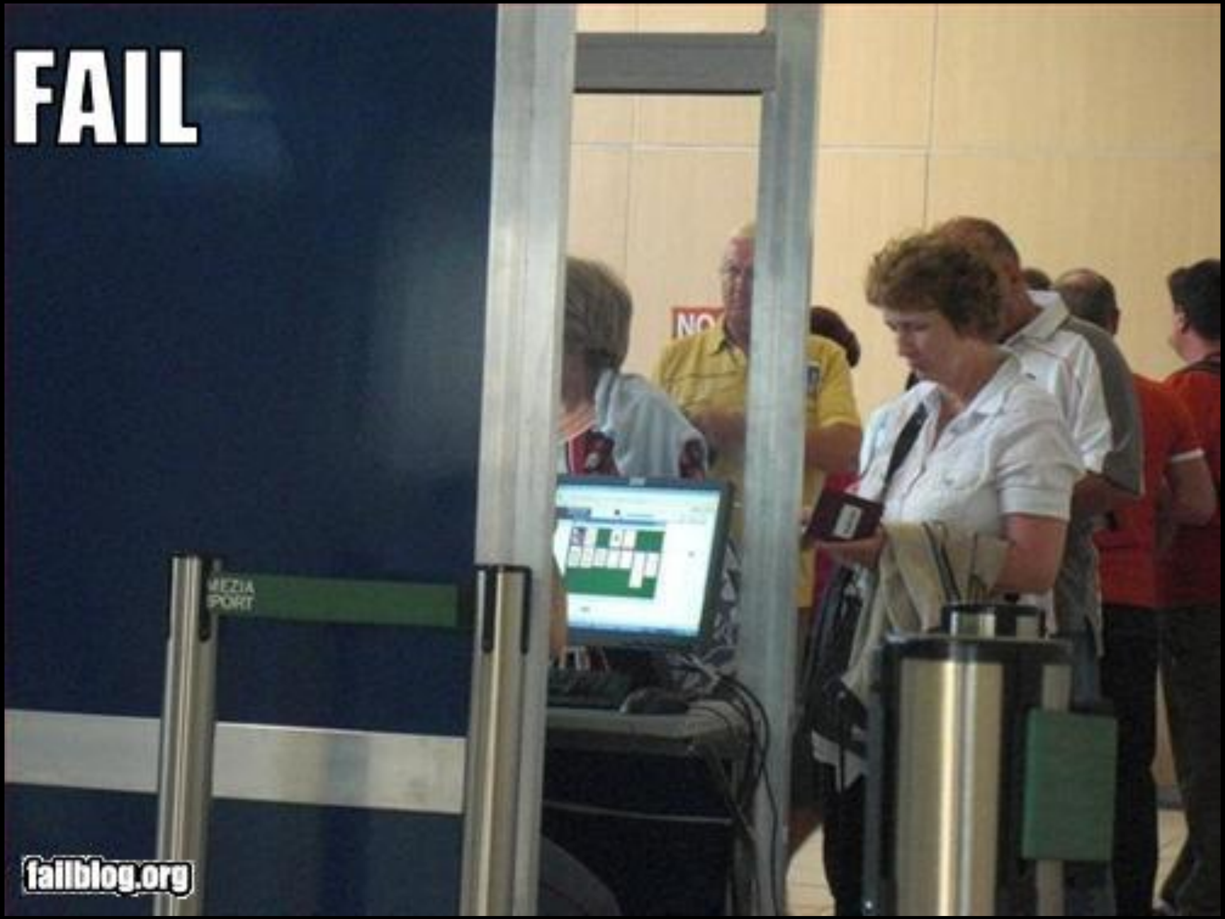


Photo: Wikimedia

- Smallpox
- Deadliest disease in history
- 1900-**2000**
  - 500 million victims died
  - 15 million per year in 60s
  - ½ of all blindness in Asia
- WHO campaign to eradicate the disease

“Security is not my problem……”

“Security really (really, really, really……..) is my problem”



“Security is my problem……but I really don’t care”

Mark Curphey rocks!

1. Process Matters

   Integrated Development Practices

   Clear Security Requirements

   Measurement of Success

2. Technology Matters

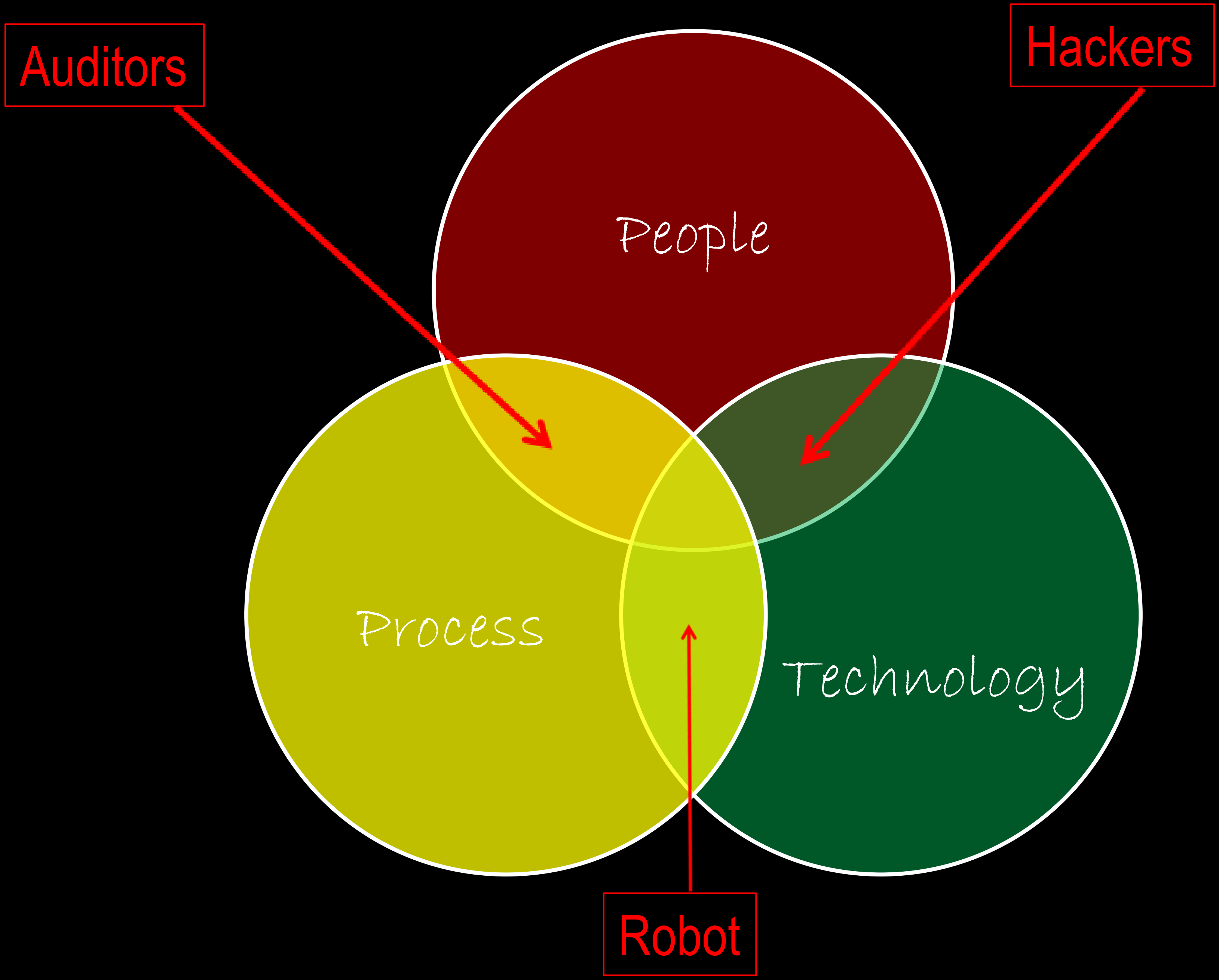
   Security Features / API's (right tool for the job)

   Tools are critical. People Don't Scale!

   Architecture is Not a Dirty Word

   Purple Dinosaurs are Everywhere

3. People Matter



Auditors

Hackers

People

Process

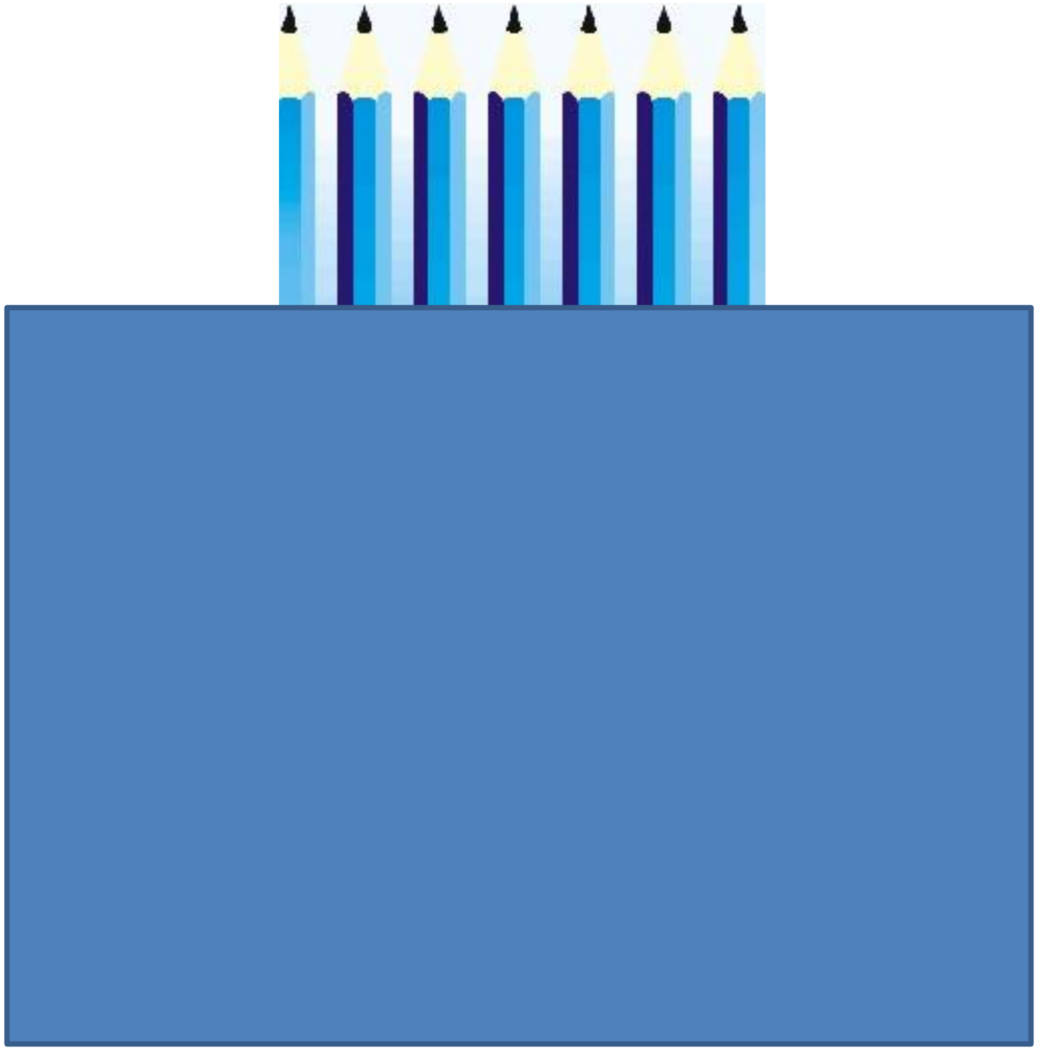
Technology

Robot

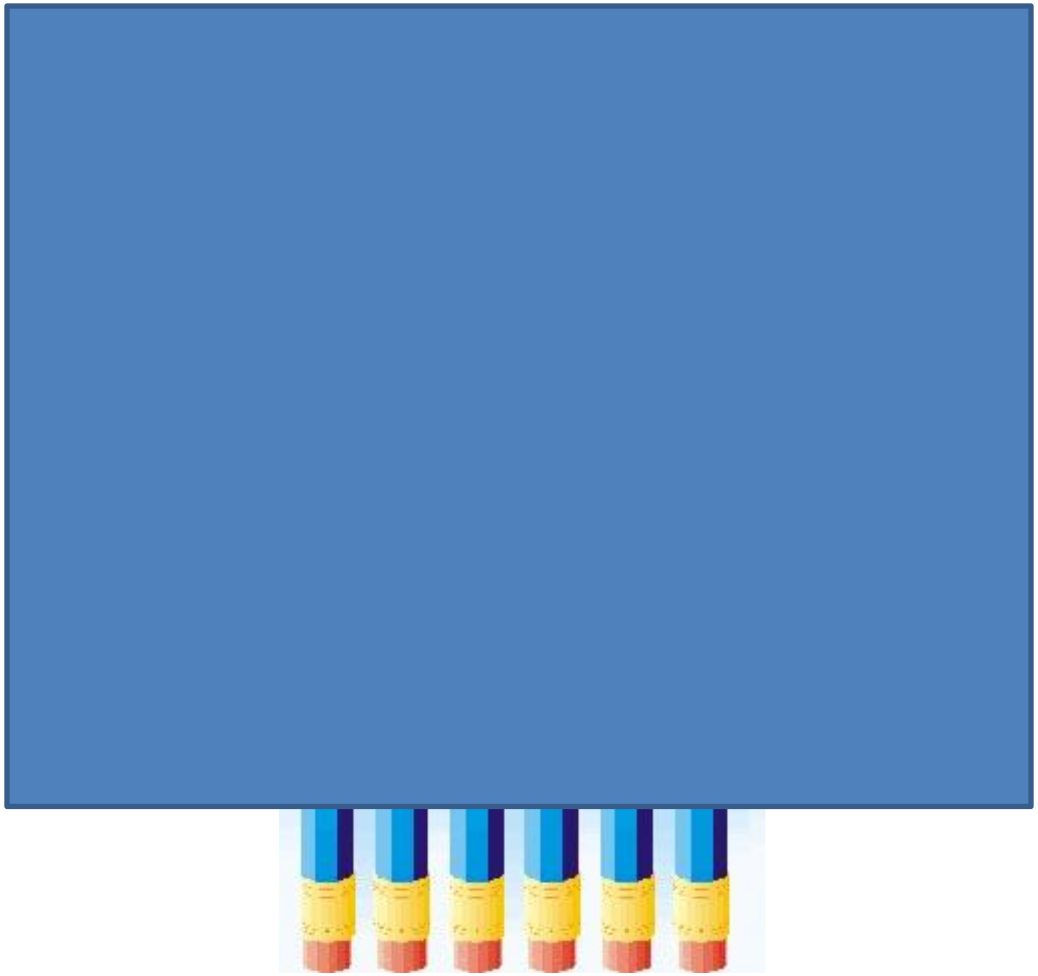
#1 – Adopt Chinese Medicine Business Model

#2 – Stop Human Pattern Matching

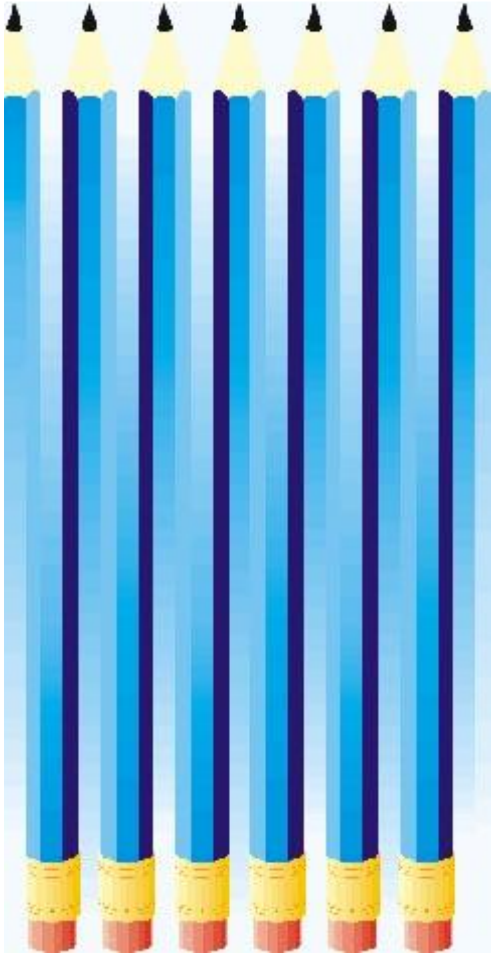
How many pencils are there in this picture?



How many pencils are there in this picture?



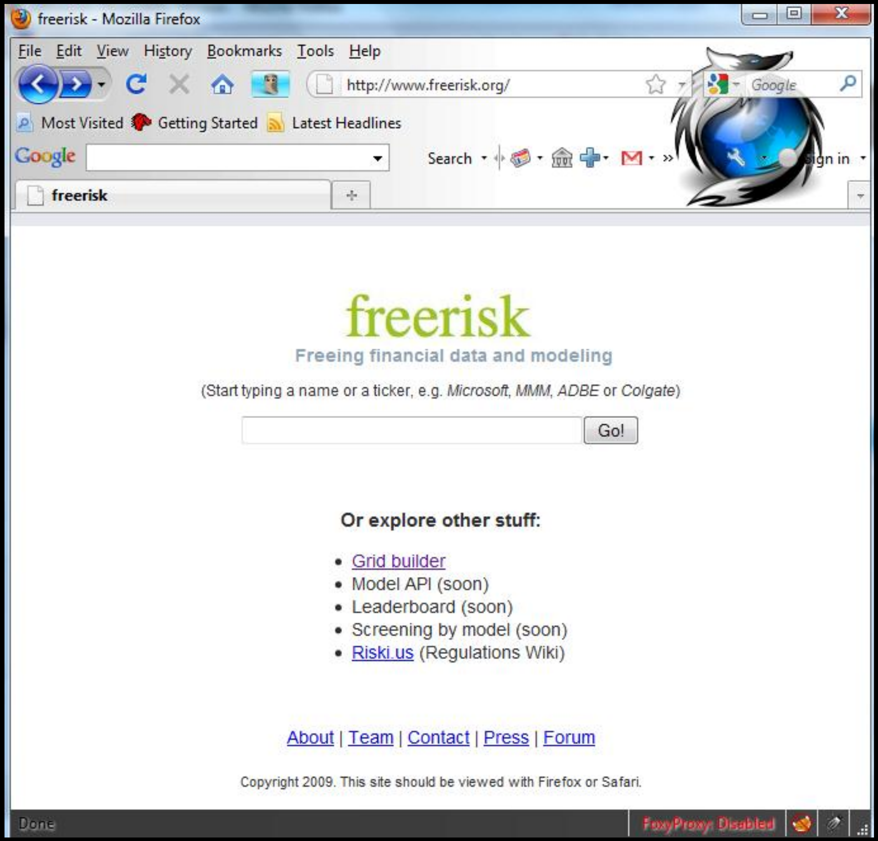
How many pencils are there in this picture?



If you are still not convinced ?

To Be Clear Computers Pattern Match (Some Things) Very Well !

# 3 Community Driven Statistical Modeling


freerisk - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.freerisk.org/
Google
Most Visited Getting Started Latest Headlines
Google
Search
Sign in
freerisk
Done
FoxyProxy: Disabled

freerisk

Freeing financial data and modeling

(Start typing a name or a ticker, e.g. *Microsoft, MMM, ADBE* or *Colgate*)

Go!

Or explore other stuff:

- Grid builder
- Model API (soon)
- Leaderboard (soon)
- Screening by model (soon)
- Riski.us (Regulations Wiki)

About | Team | Contact | Press | Forum

Copyright 2009. This site should be viewed with Firefox or Safari.

Alpha geeks Jesper Andersen (left) and Toby Segaran

Photo: Joe Pugliese

Wine Quality = 12.145 + .00117 * winter rainfall + .0614 average growing season - .00386 harvest rainfall

Where is the security equivalent ?

$$\Pr[T_A < 1, T_B < 1] = \phi_2(\phi^{-1}(F_A(1)), \phi^{-1}(F_B(1)), \gamma)$$

Security is a function of
$S = ƒ(\_\_\_\_)$ …

$S = ƒ(°WFF)$

Degrees of Warm Fuzzy Feeling

$S=f(p,d)+Rn$

Prayer, Denial) + Number of Days till Retirement

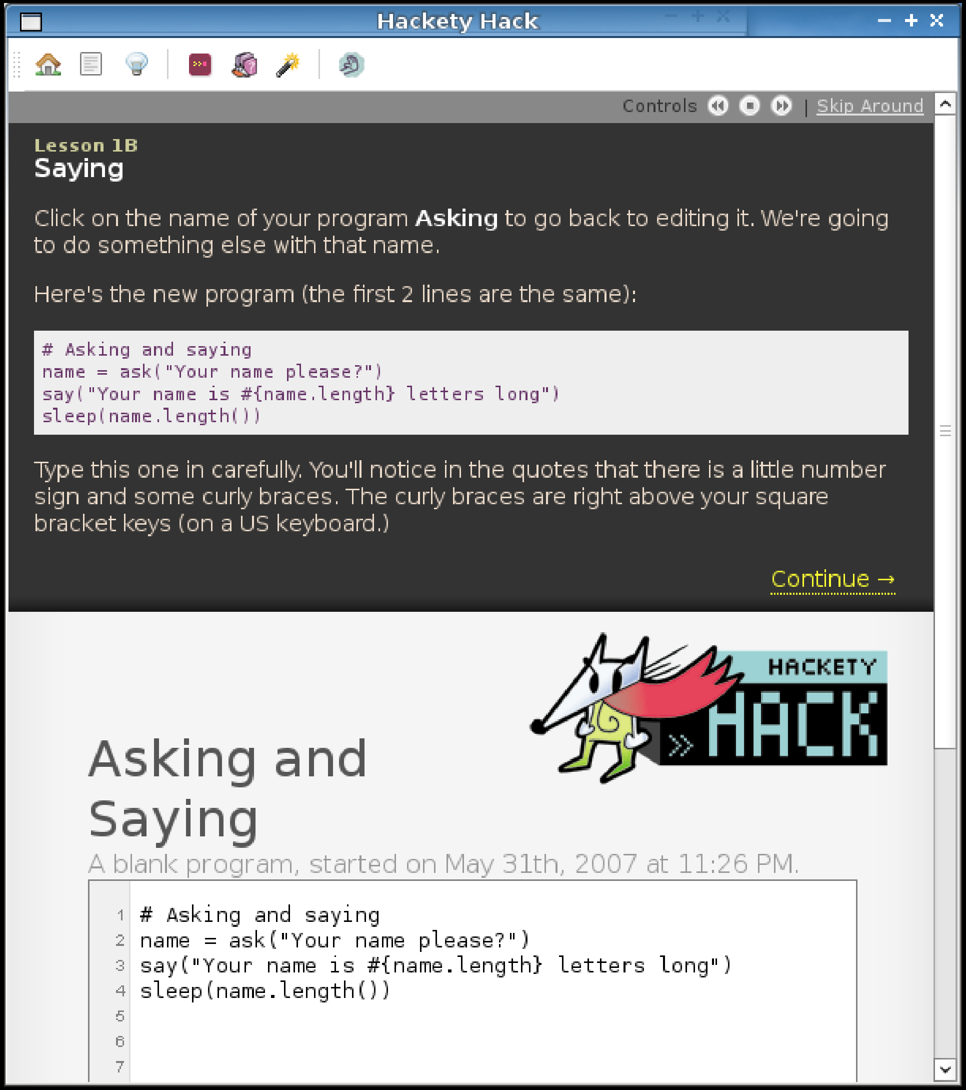
$S=f(n)$

Where n is the number of security guys you know

$S=f(1/n)$

Where n is the number of security standards documents you have read

# 4 – Teach Kids Computer Security



Lesson 1B

Saying

Click on the name of your program **Asking** to go back to editing it. We're going to do something else with that name.

Here's the new program (the first 2 lines are the same):

```
# Asking and saying
name = ask("Your name please?")
say("Your name is #{name.length} letters long")
sleep(name.length())
```

Type this one in carefully. You'll notice in the quotes that there is a little number sign and some curly braces. The curly braces are right above your square bracket keys (on a US keyboard.)

Asking and Saying

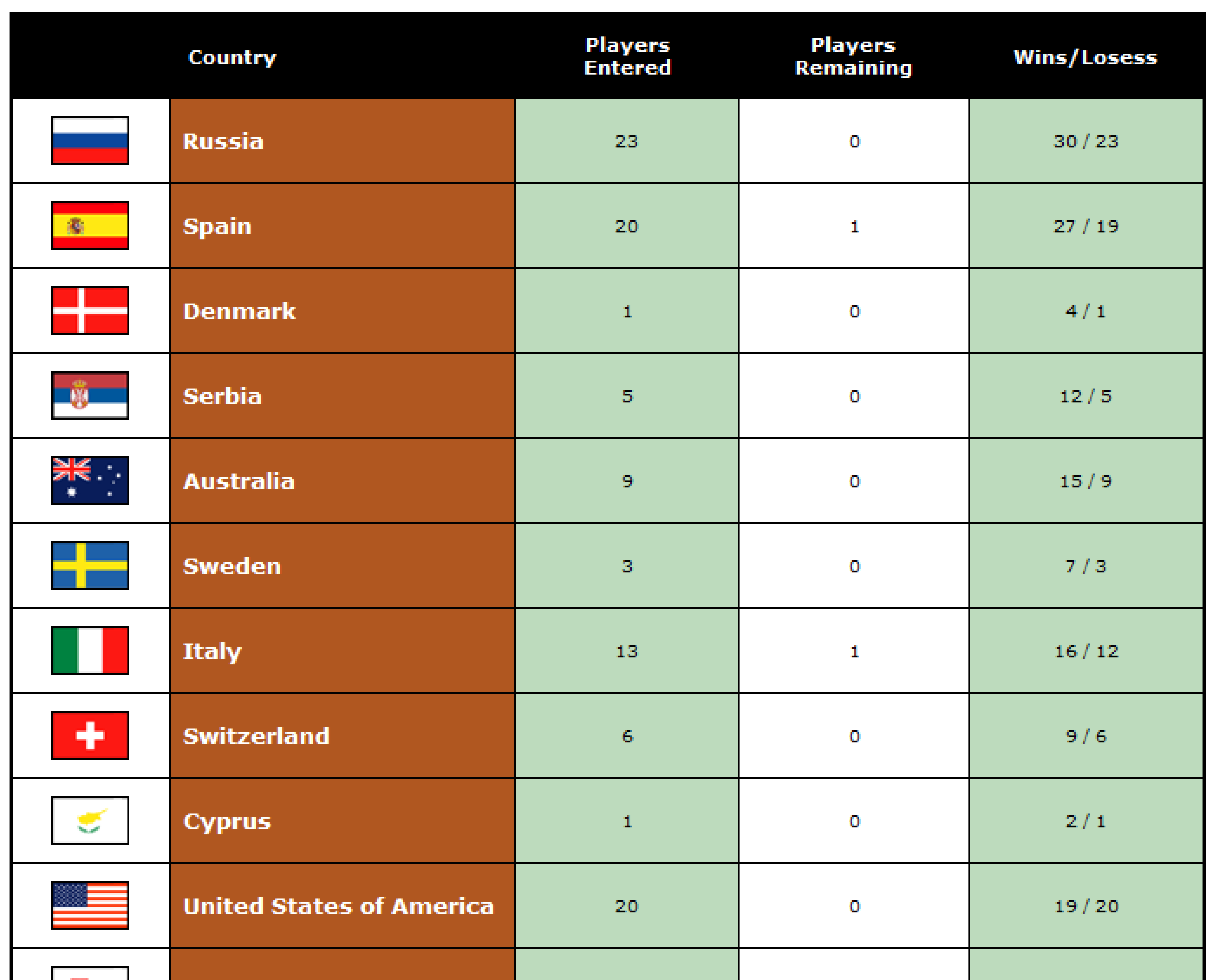
A blank program, started on May 31th, 2007 at 11:26 PM.

```
# Asking and saying
name = ask("Your name please?")
say("Your name is #{name.length} letters long")
sleep(name.length())
```

#5 Make Developing Countries Centers for Security Excellence

Make Me Stop and Take a Photo of The Audience

# 6 – Make Hacking a Competitive Sport



Country		Players Entered	Players Remaining	Wins/Losess
🇷🇺	Russia	23	0	30 / 23
🇪🇸	Spain	20	1	27 / 19
🇩🇰	Denmark	1	0	4 / 1
🇷🇸	Serbia	5	0	12 / 5
🇦🇺	Australia	9	0	15 / 9
🇸🇪	Sweden	3	0	7 / 3
🇮🇹	Italy	13	1	16 / 12
🇨🇭	Switzerland	6	0	9 / 6
🇨🇾	Cyprus	1	0	2 / 1
🇺🇸	United States of America	20	0	19 / 20

# 7 – Connected Information Security Framework

#8- Embrace Design Driven Security

“We must reward the builders and the breakers”

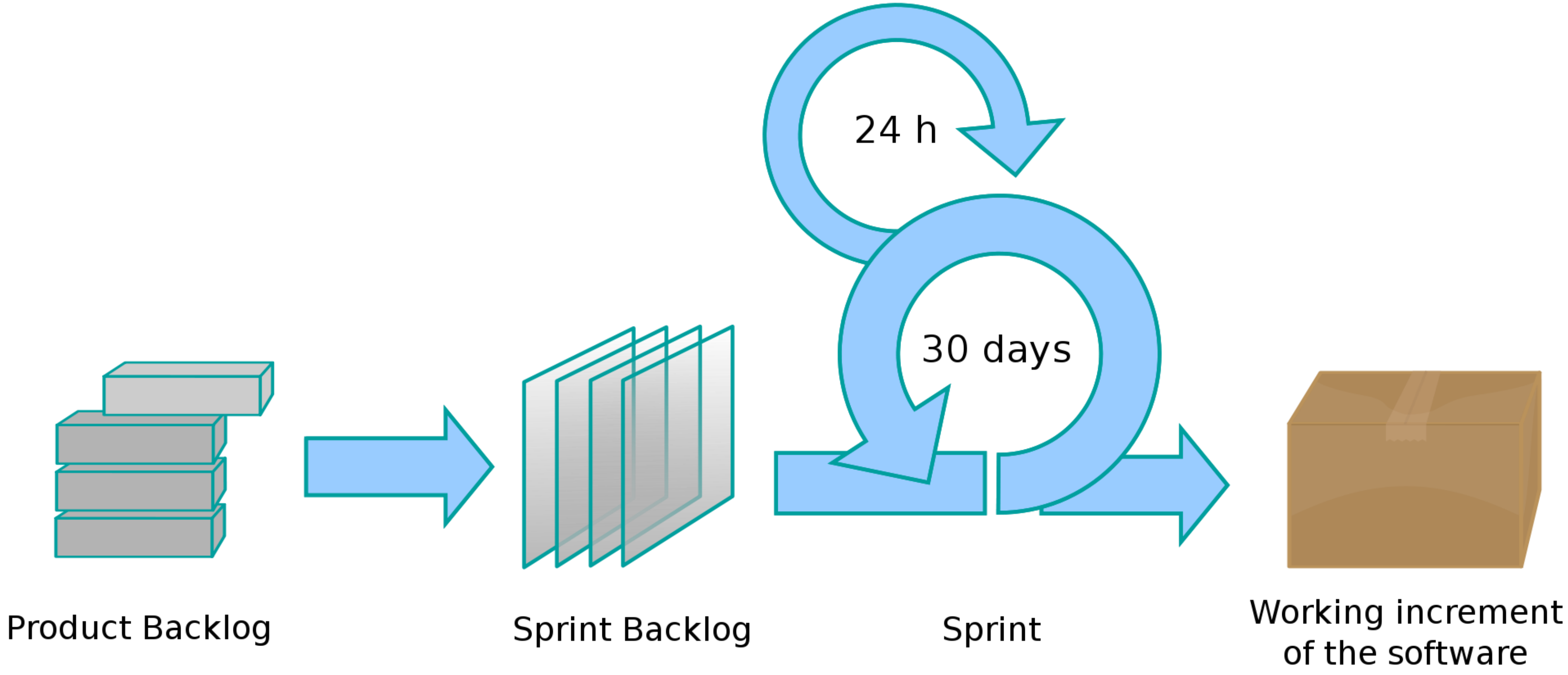
#9 Crowd Source Access Control

#10 Adopt Agile Mindset

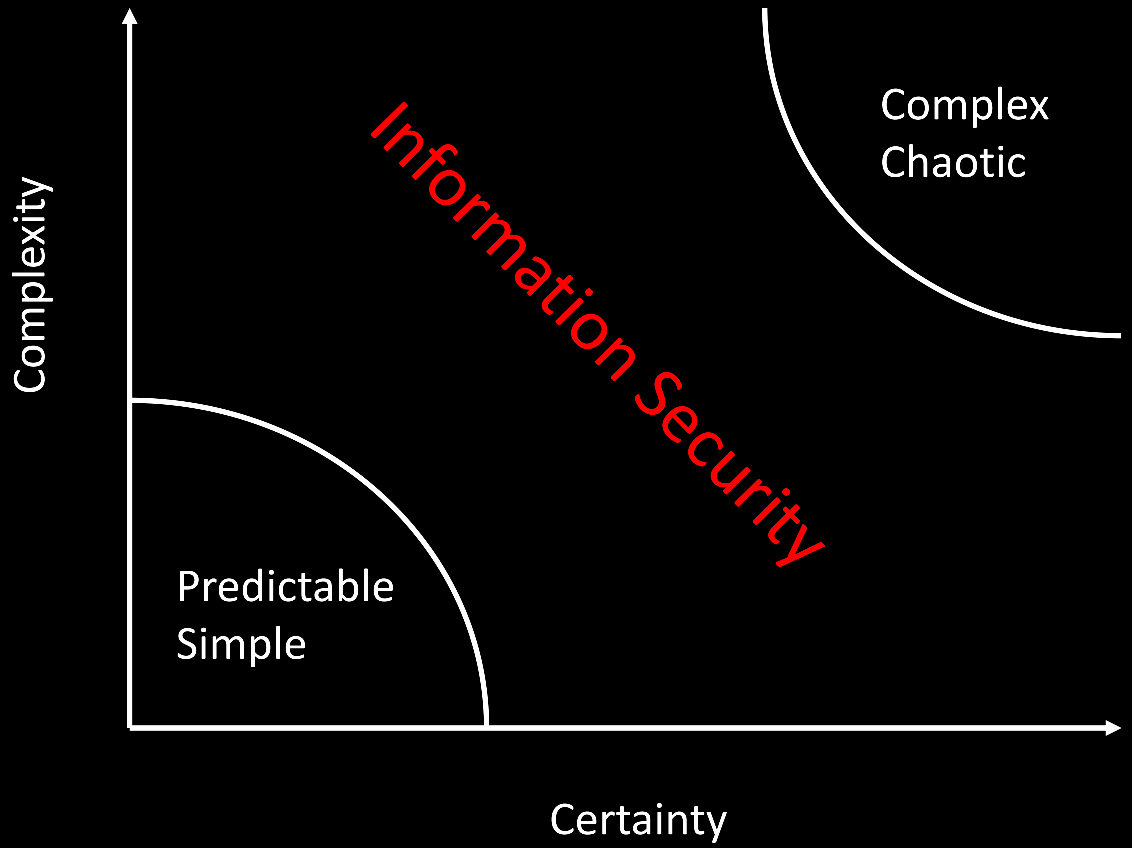
The Agile Manifesto - http://agilemanifesto.org/

New thinking	versus	old thinking
Individuals and interactions	over	processes and tools
Working software	over	comprehensive documentation
Customer collaboration	over	contract negotiation
Responding to change	over	following a plan

“That is, while there is value in the items on the right, we value the items on the left more.”

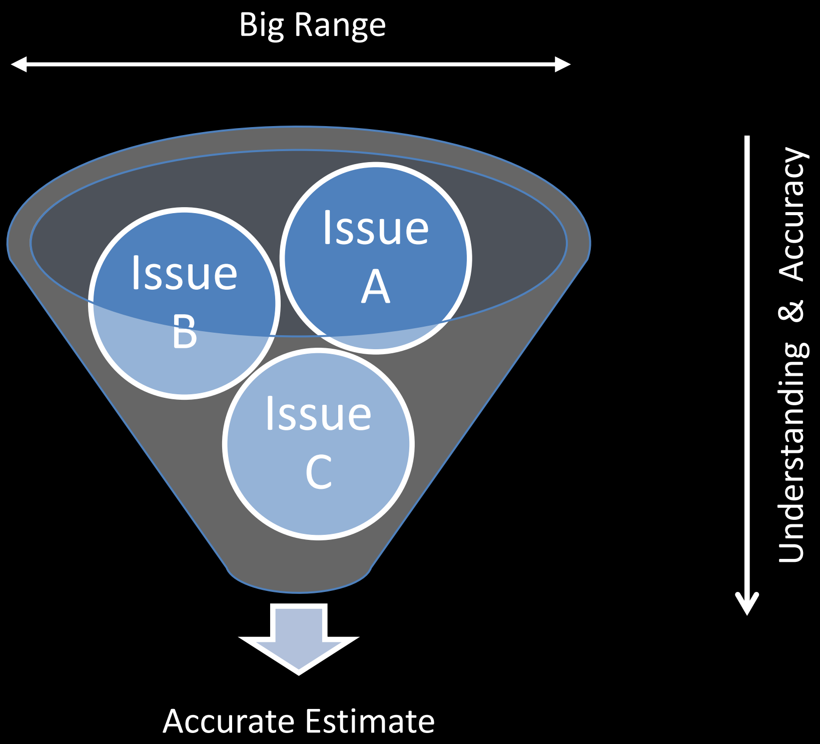


"By embracing constraints you can do the most important half of a job, rather than a half-assed job"

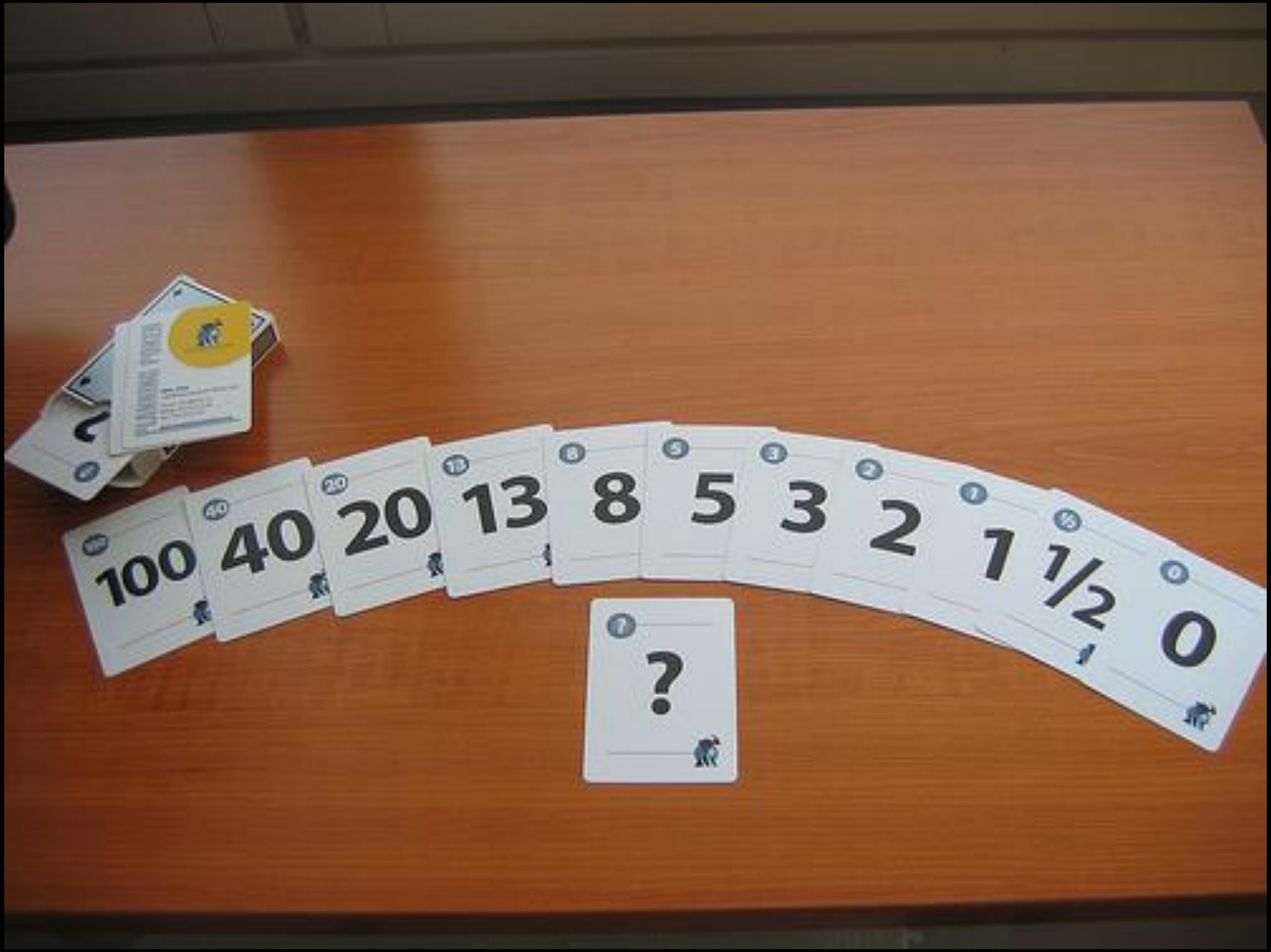


"The Ralph Stacey Diagram"

The Truth About Estimation



10
55
60
5
50
10
45
15
40
20
35
30
25


PLANNING POKER
100
40
20
13
8
5
3
2
1
½
0
?

Common Statement: “But Agile is not for the Enterprise.”

Factual Answer: “Enterprise? – A colossal spaceship from the 80’s flown by people with bad taste: Highly advanced, but purely fictional”

10 Crazy Ideas That Might Just Change the State of the Security Industry

# 1 – Adopt the Chinese Medicine Business Model
# 2 – Stop Human Pattern Matching
# 3 – Community Driven Statistical Modeling
# 4 – Teach Kids Security
# 5 – Make Developing Countries Security COE's
# 6 – Make Hacking a Competitive Sport
# 7 – Build a Connected Information Security Framework
# 8 – Design Driven Security
# 9 – Crowd Source Access Control
# 10 – Adopt Agile Methodologies

It doesn’t have to be this hard!

Photo: Theorris, Myth of Sisyphus (detail): Captain Sisyphus http://flickr.com/photos/signifying/2073074572/

@curphey