Me and my digital shadow: Protecting and detecting on the social web

David Porter

Resilient Thinking

Session ID: STAR-209

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

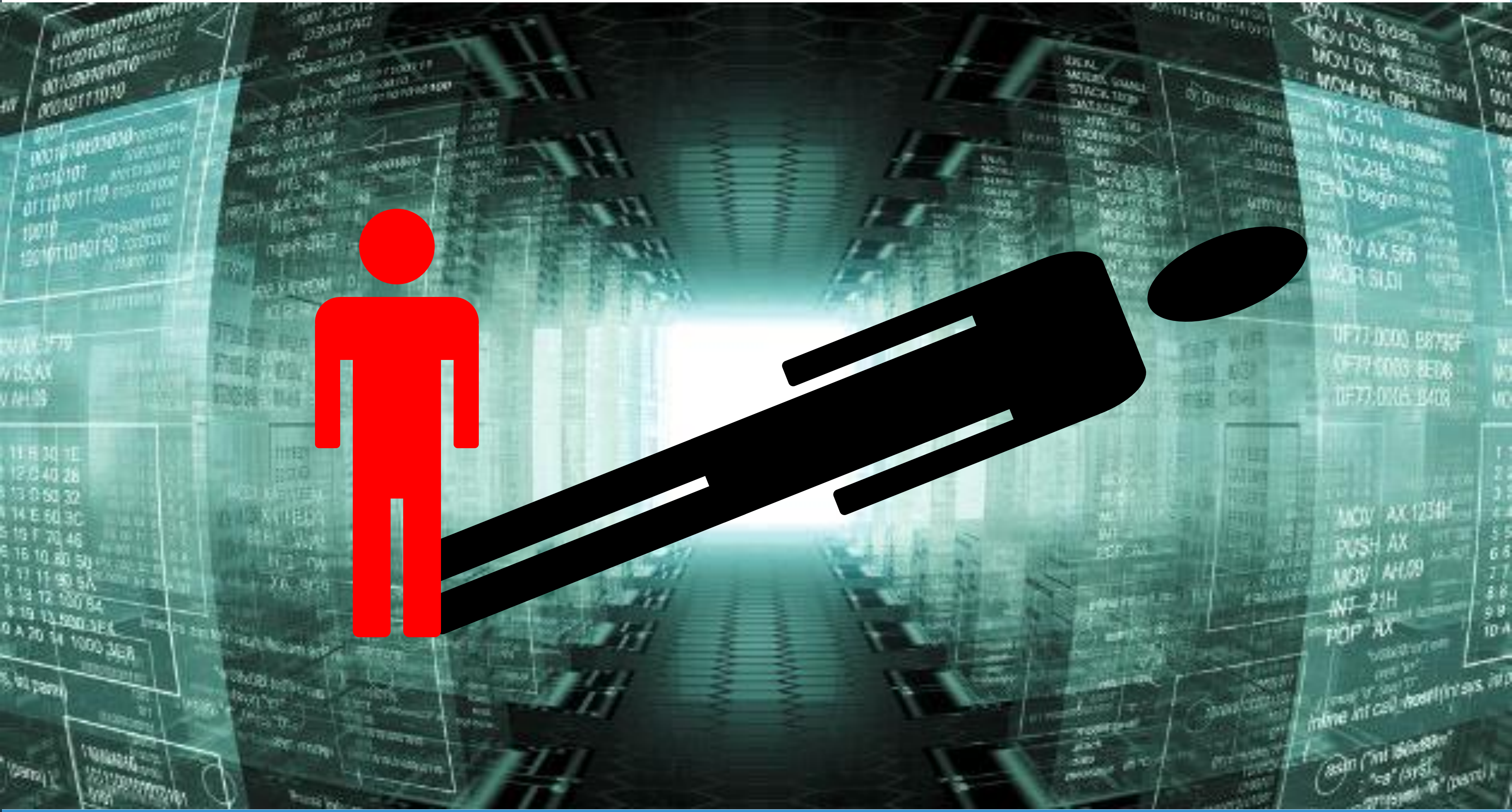
The rise of the social web

1bn Facebook messages per day (955m users)

340m Tweets per day (140m-500m users)

Source: Facebook 16 June 2012/Twitter 21 March 2012/Semiocast 30 July 2012

Digital shadows: friend or foe?



The darker side of socialising

NON-COMPLIANCE

DISCLOSURE

DEFAMATION

EXPOSURE

MISINFORMATION

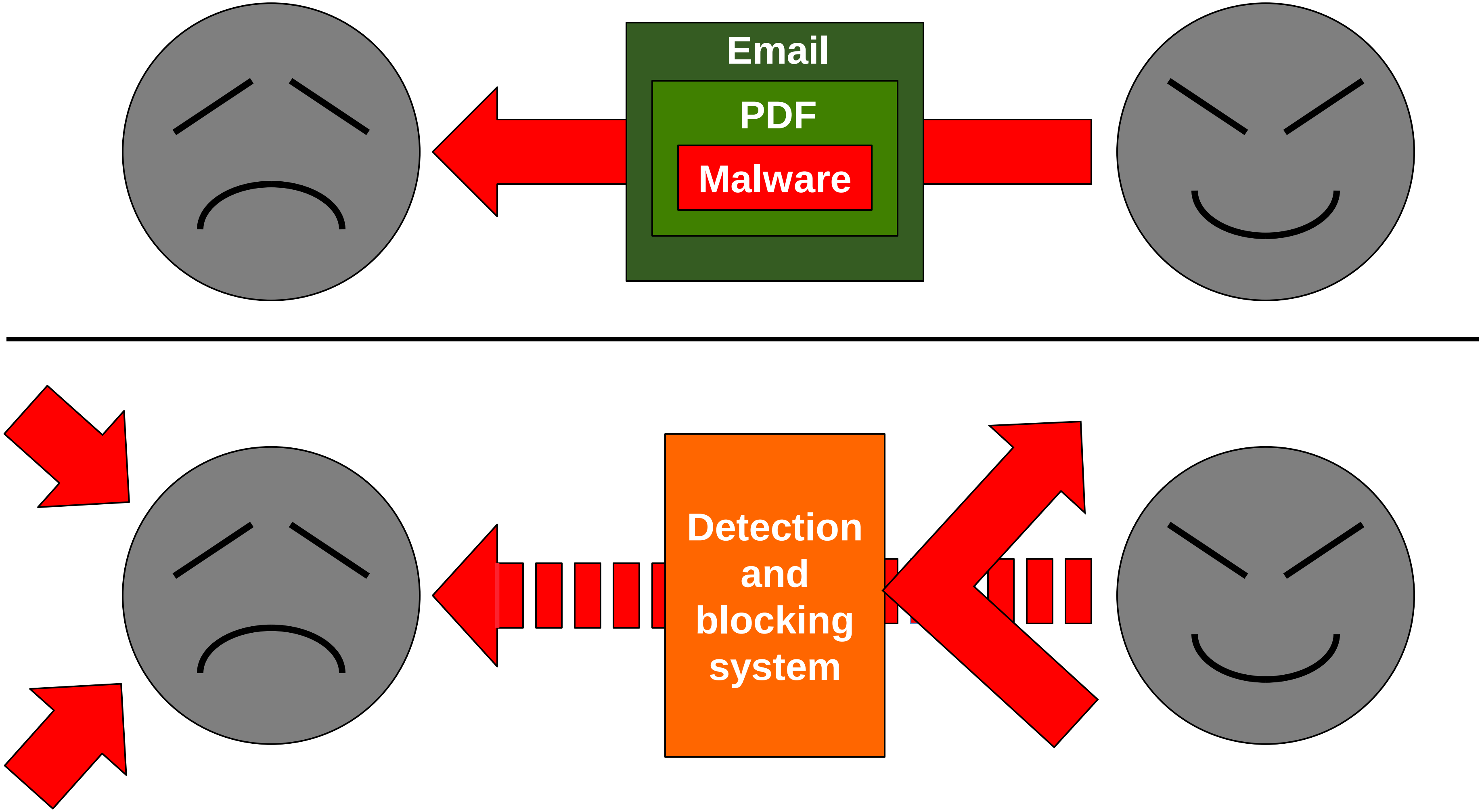
THEFT

FRAUD

THREAT

> *"Credible threats to cyber security of an unprecedented scale, diversity and complexity"*
>
> Iain Lobban, Director, GCHQ
> 5 September 2012

Greater focus on attacks than actors



Is there more to this than high fences?

Coming up…

Actors on a stage

Secrets in the shadows

A mightier sword?

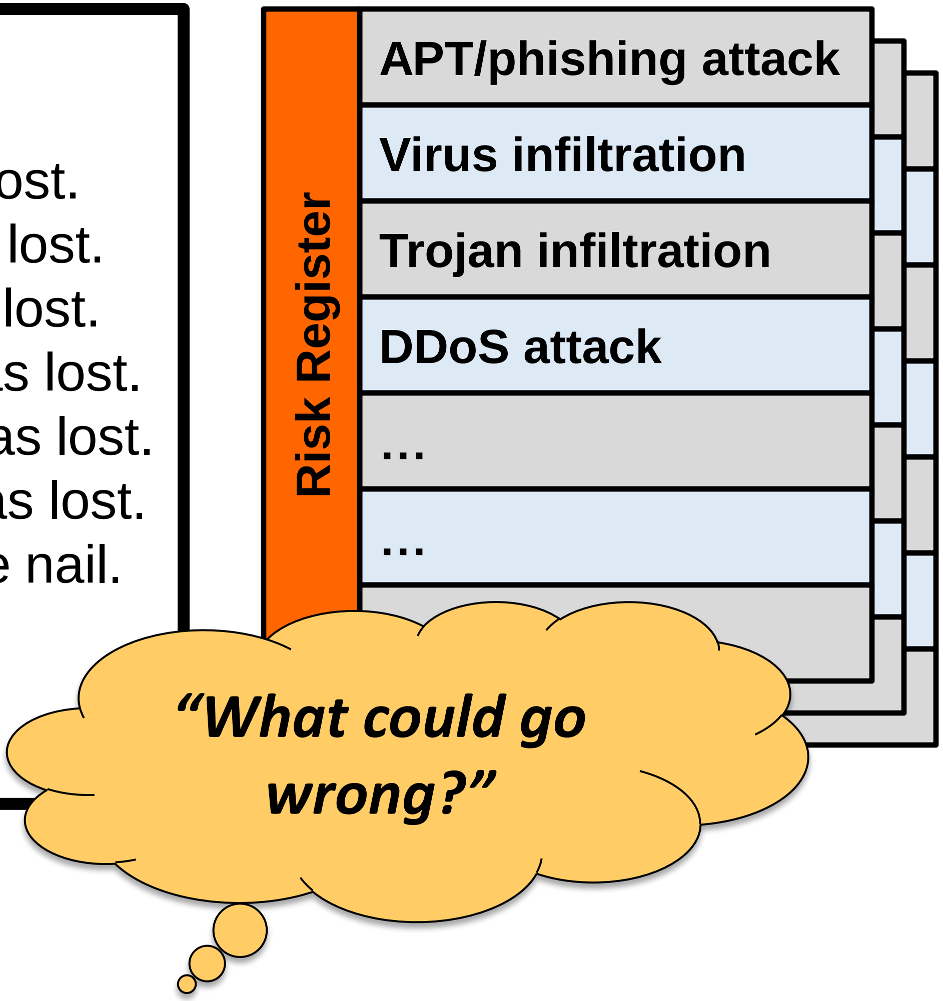
Actors on a stage

Problem-driven risk modelling

For want of a Nail

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a horseshoe nail.

George Herbert
Outlandish Proverbs, 1640



Risk Register

- **APT/phishing attack**
- **Virus infiltration**
- **Trojan infiltration**
- **DDoS attack**
- **…**
- **…**

"What could go wrong?"

An alternative definition of risk

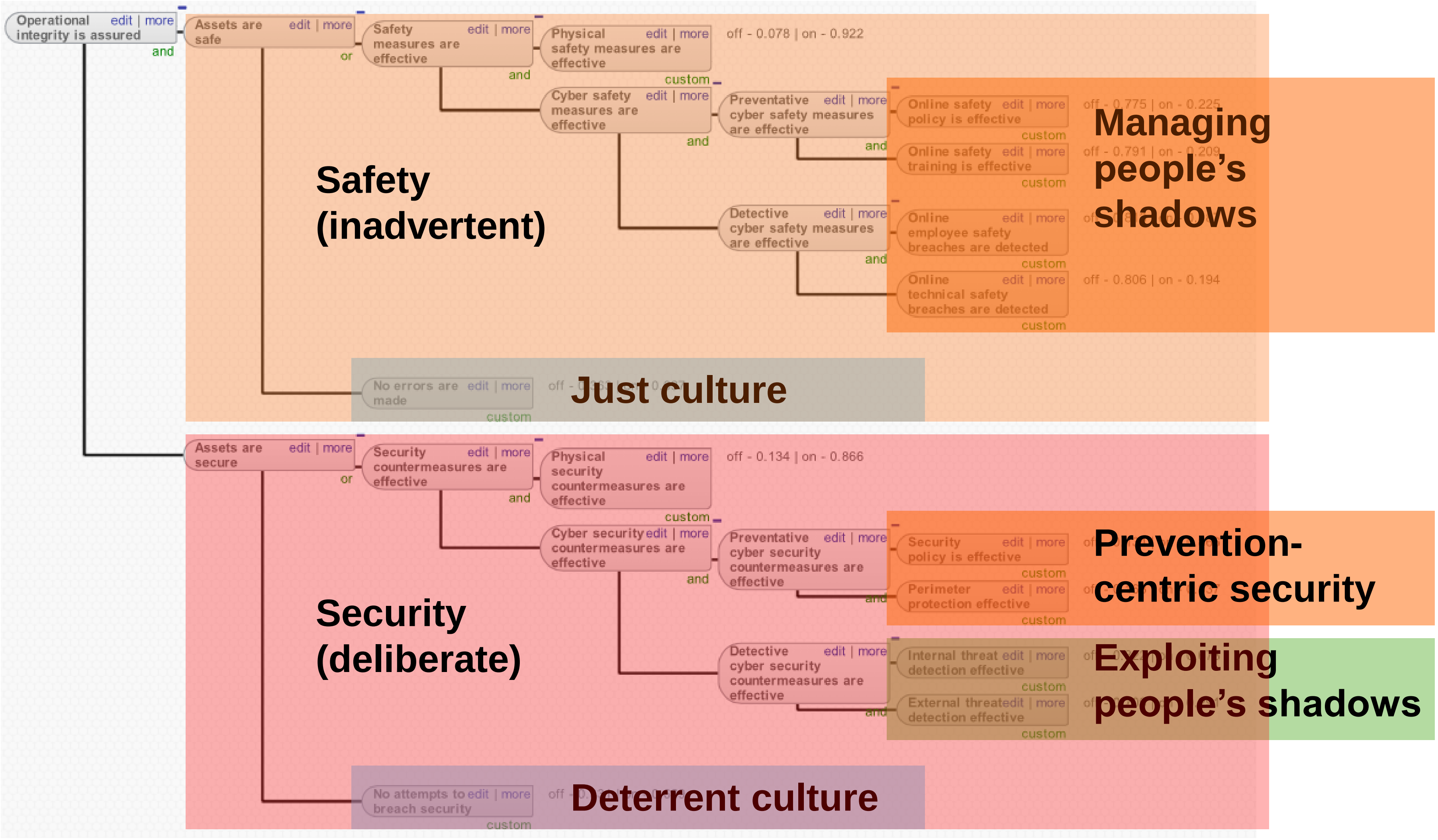
“Risk: the degree to which the chance of achieving our goals depends on things we cannot control, predict or understand”

“What do we need to succeed?”

Resilient Thinking

Source: Gordon, J., *Dependency modelling and understanding risks to the infrastructure*, 2011

Goal-driven risk modelling


Operational integrity is assured
edit | more
and
Assets are safe
edit | more
or
Safety measures are effective
edit | more
and
Physical safety measures are effective
edit | more
custom
off - 0.078 | on - 0.922
Cyber safety measures are effective
edit | more
and
Preventative cyber safety measures are effective
edit | more
and
Online safety policy is effective
edit | more
custom
off - 0.775 | on - 0.225
Online safety training is effective
edit | more
custom
off - 0.791 | on - 0.209
Detective cyber safety measures are effective
edit | more
and
Online employee safety breaches are detected
edit | more
custom
Online technical safety breaches are detected
edit | more
custom
off - 0.806 | on - 0.194
No errors are made
edit | more
custom
Assets are secure
edit | more
or
Security countermeasures are effective
edit | more
and
Physical security countermeasures are effective
edit | more
custom
off - 0.134 | on - 0.866
Cyber security countermeasures are effective
edit | more
and
Preventative cyber security countermeasures are effective
edit | more
and
Security policy is effective
edit | more
custom
Perimeter protection effective
edit | more
custom
Detective cyber security countermeasures are effective
edit | more
and
Internal threat detection effective
edit | more
custom
External threat detection effective
edit | more
custom
No attempts to breach security
edit | more
custom

Safety (inadvertent)

Managing people's shadows

Just culture

Security (deliberate)

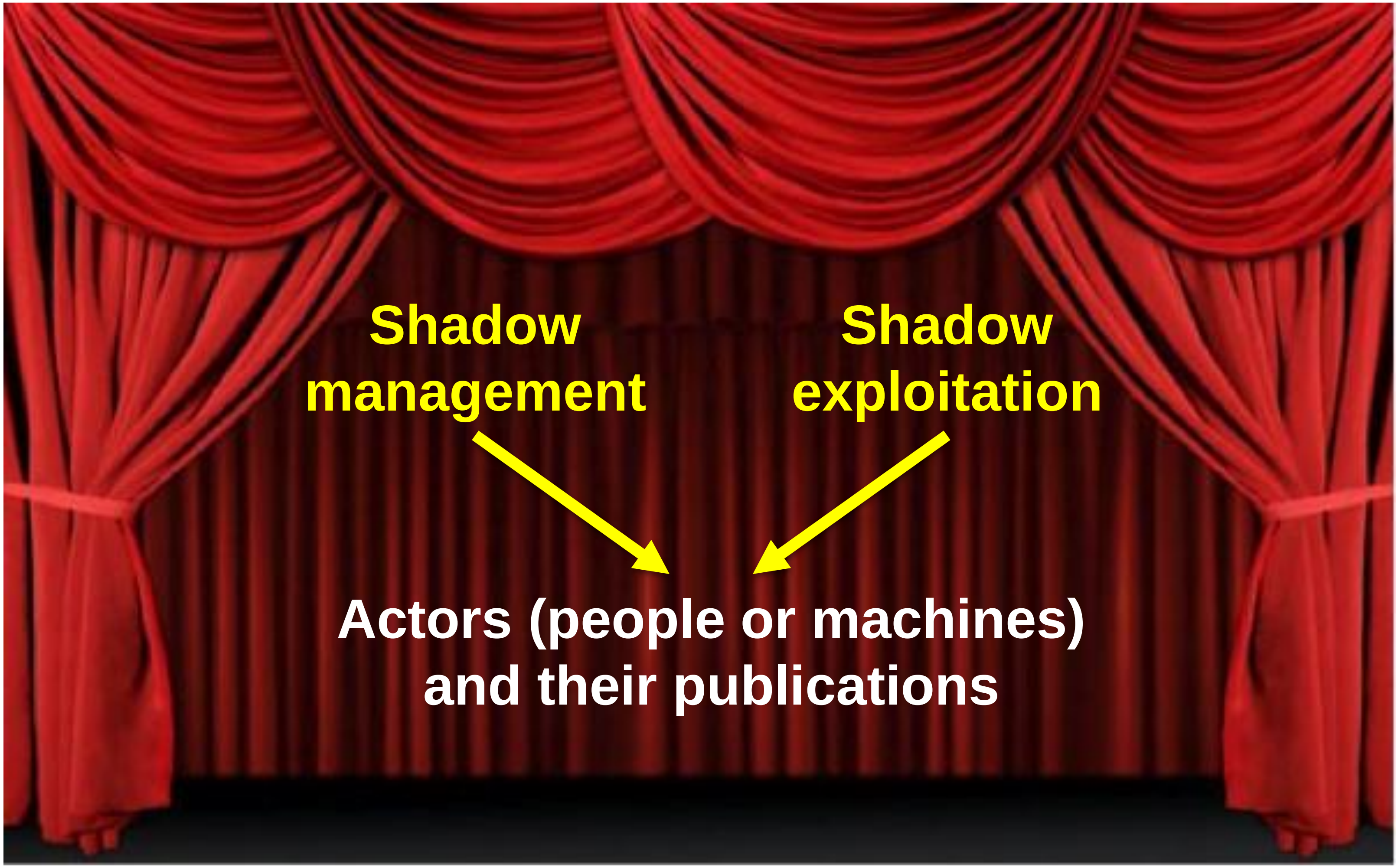
Prevention-centric security

Exploiting people's shadows

Deterrent culture

iDepend dependency modelling facility courtesy of Intradependency (www.intradependency.com)

A new line of enquiry



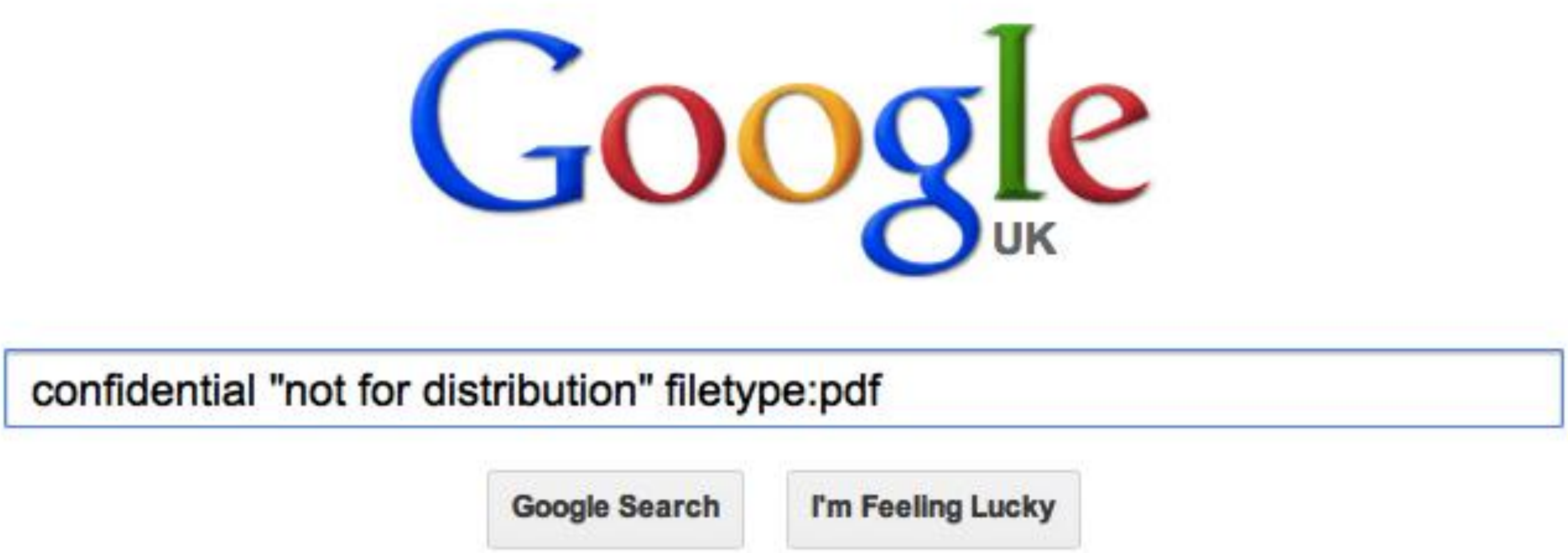
Shadow management

Shadow exploitation

Actors (people or machines) and their publications

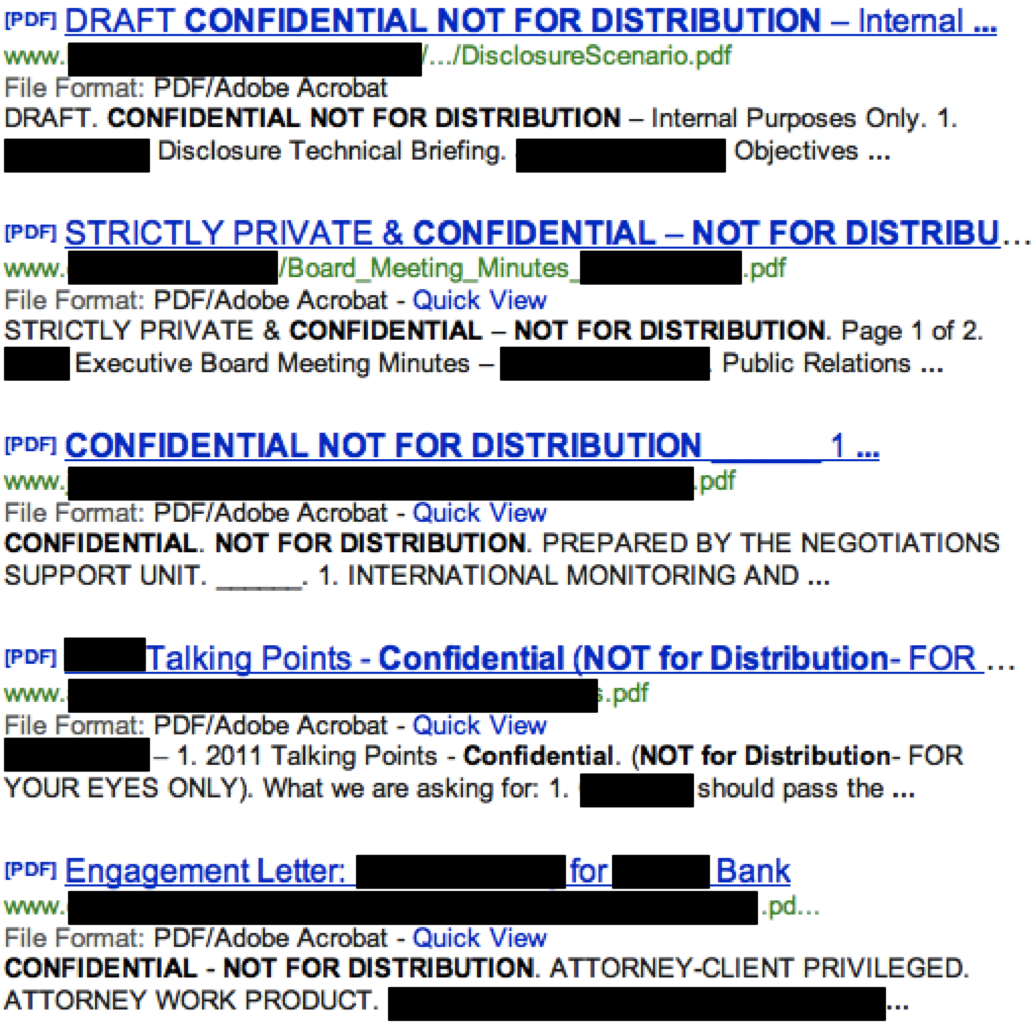
Secrets in the shadows

Ever tried this?



confidential "not for distribution" filetype:pdf

Not so confidential



[PDF] DRAFT **CONFIDENTIAL NOT FOR DISTRIBUTION** – Internal ...
www.[redacted]/.../DisclosureScenario.pdf
File Format: PDF/Adobe Acrobat
DRAFT. **CONFIDENTIAL NOT FOR DISTRIBUTION** – Internal Purposes Only. 1.
[redacted] Disclosure Technical Briefing. [redacted] Objectives ...

[PDF] STRICTLY PRIVATE & **CONFIDENTIAL** – **NOT FOR DISTRIBU**...
www.[redacted]/Board_Meeting_Minutes_[redacted].pdf
File Format: PDF/Adobe Acrobat - Quick View
STRICTLY PRIVATE & **CONFIDENTIAL** – **NOT FOR DISTRIBUTION**. Page 1 of 2.
[redacted] Executive Board Meeting Minutes – [redacted] Public Relations ...

[PDF] **CONFIDENTIAL NOT FOR DISTRIBUTION** ________ 1 ...
www.[redacted].pdf
File Format: PDF/Adobe Acrobat - Quick View
CONFIDENTIAL. **NOT FOR DISTRIBUTION**. PREPARED BY THE NEGOTIATIONS SUPPORT UNIT. ______. 1. INTERNATIONAL MONITORING AND ...

[PDF] [redacted] Talking Points - **Confidential (NOT for Distribution**- FOR ...
www.[redacted].pdf
File Format: PDF/Adobe Acrobat - Quick View
[redacted] – 1. 2011 Talking Points - **Confidential**. (**NOT for Distribution**- FOR YOUR EYES ONLY). What we are asking for: 1. [redacted] should pass the ...

[PDF] Engagement Letter: [redacted] for [redacted] Bank
www.[redacted].pd...
File Format: PDF/Adobe Acrobat - Quick View
CONFIDENTIAL - **NOT FOR DISTRIBUTION**. ATTORNEY-CLIENT PRIVILEGED. ATTORNEY WORK PRODUCT. [redacted]...

Preparation is everything

90%

The percentage of a hacker's* time spent on hostile reconnaissance

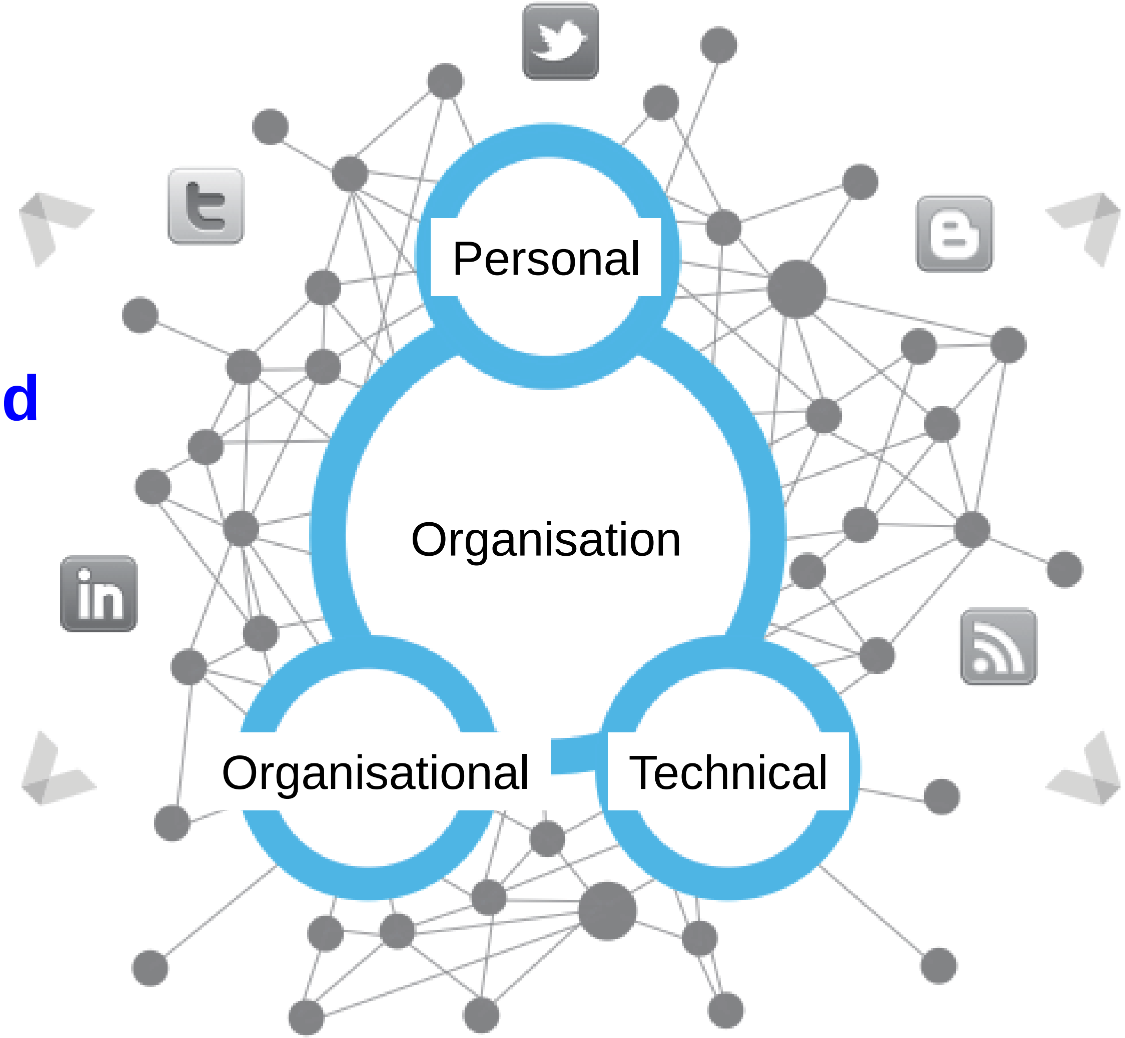
Certified Ethical Hacker Program

(*or a journalist, recruiter or competitor)

Source: International Council of Electronic Commerce Consultants (EC-Council), 2012

Components of a digital shadow

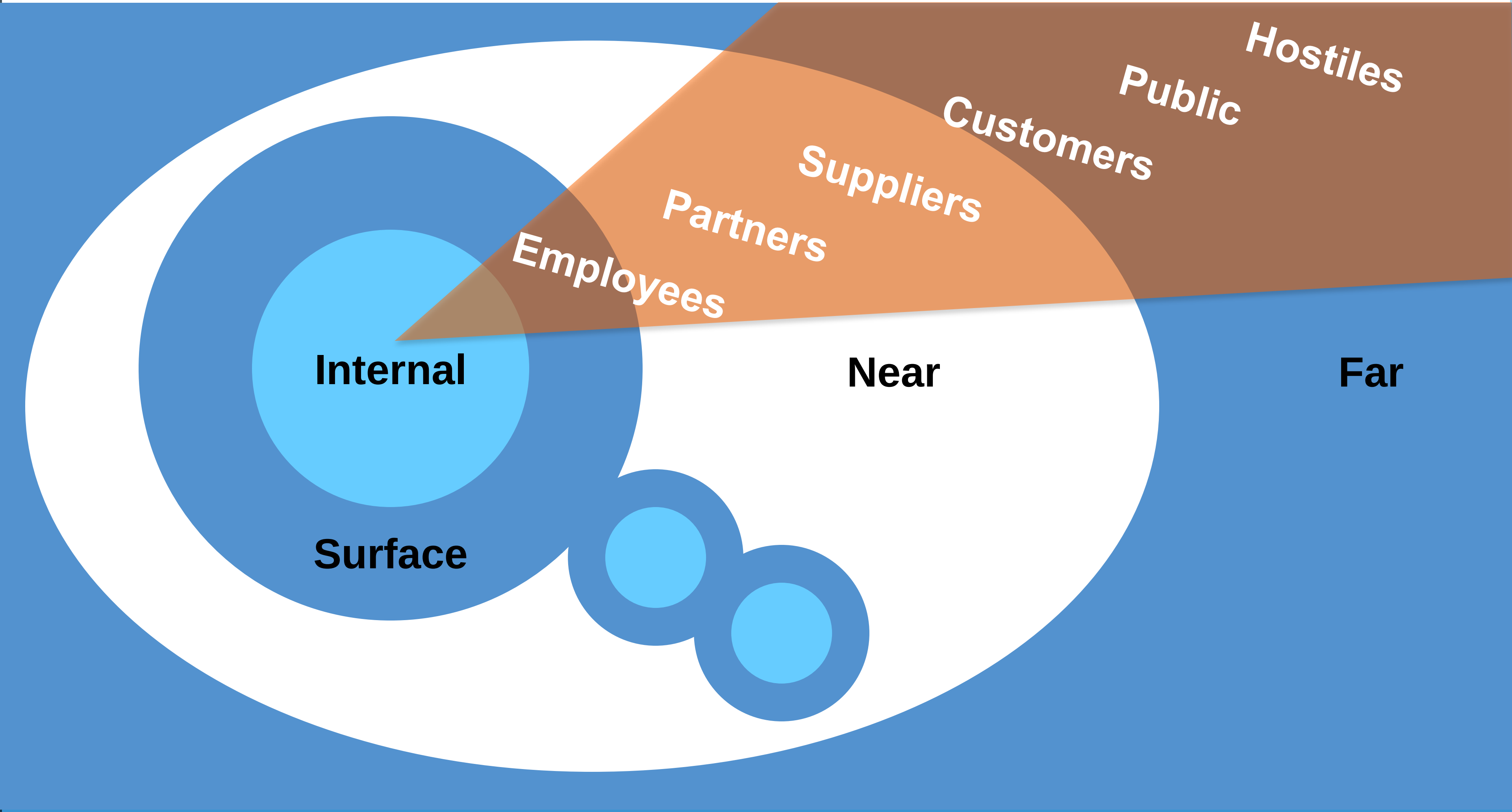
Information un-intentionally exposed that may leave an organisation open to compromise, attack or embarrassment



Resilient Thinking

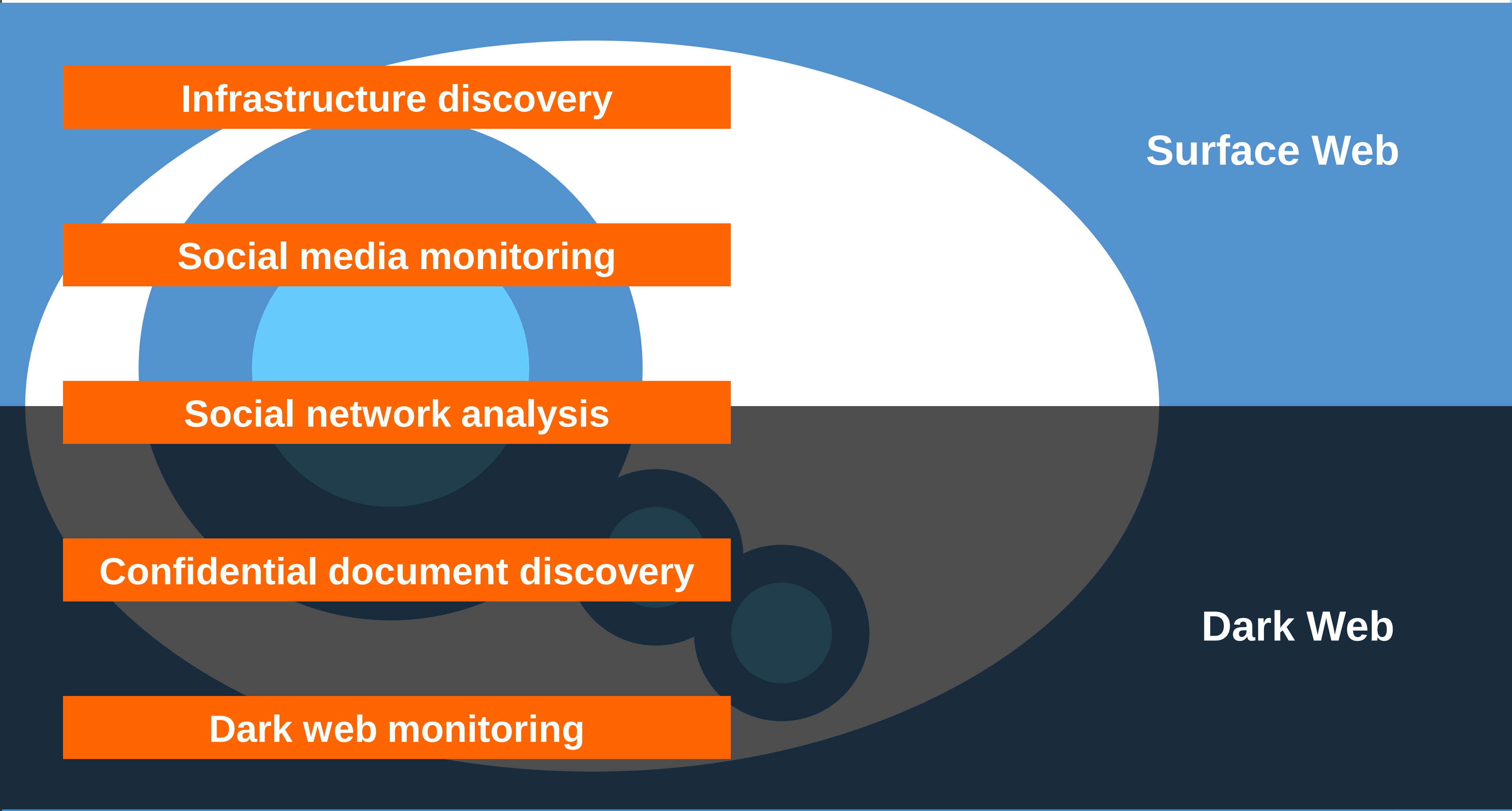
Source: Digital Shadows © Digital Shadows 2012 (www.digitalshadows.com)

Shadow intelligence model



Source: Digital Shadows © Digital Shadows 2012 (www.digitalshadows.com)

Automated discovery and monitoring



Infrastructure discovery

Social media monitoring

Social network analysis

Confidential document discovery

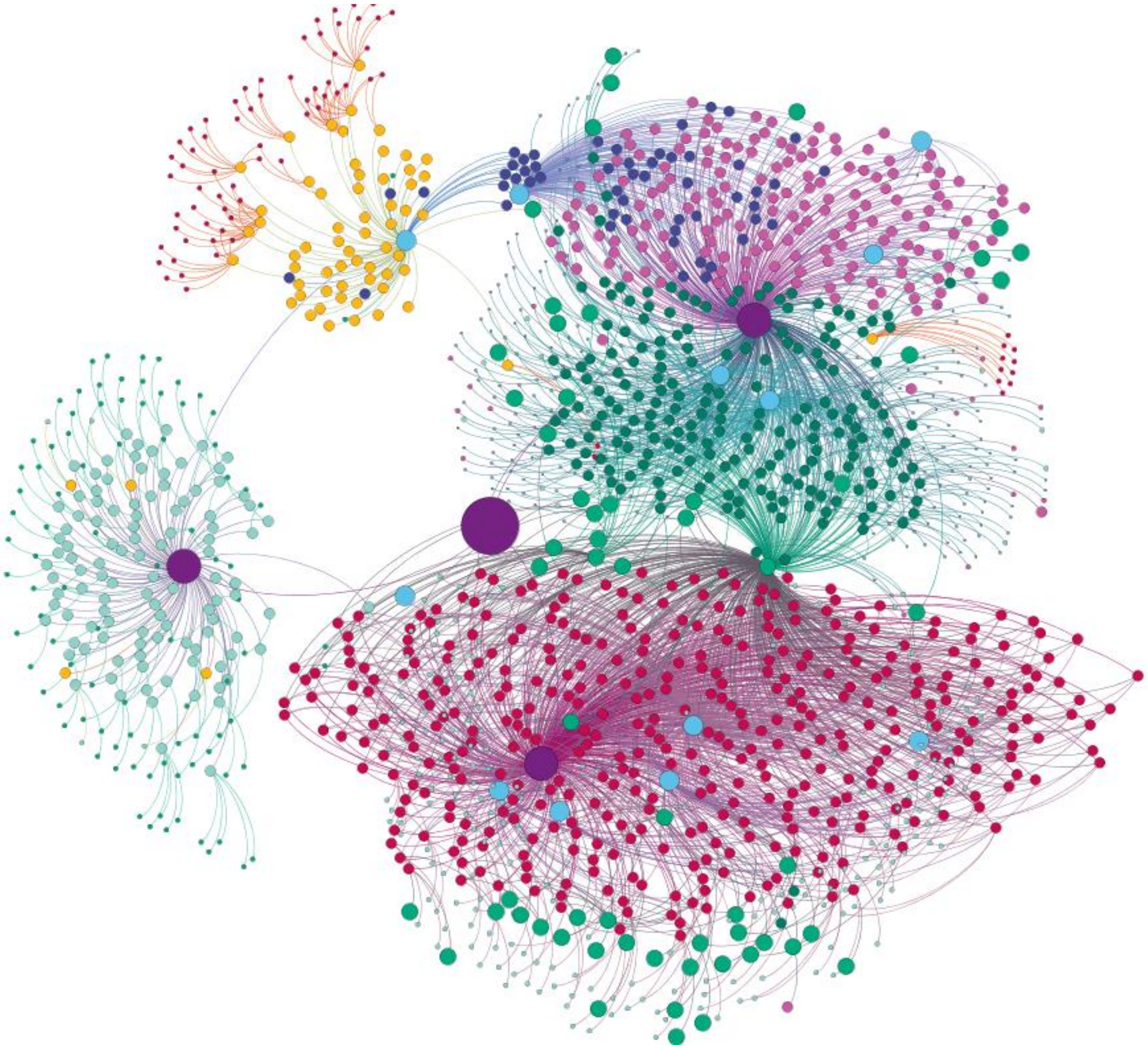
Dark web monitoring

Surface Web

Dark Web

Source: Digital Shadows © Digital Shadows 2012 (www.digitalshadows.com)

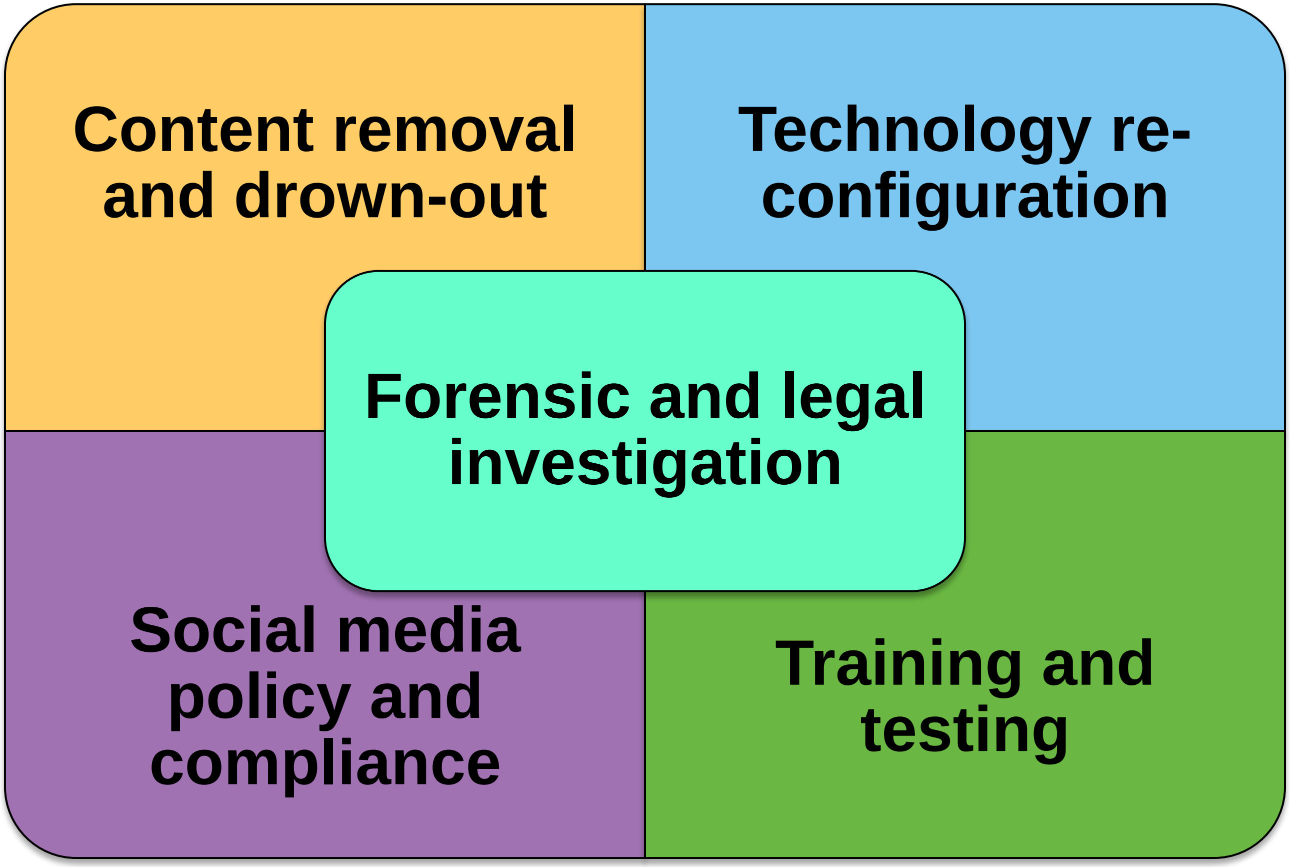
Visualising the shadow



- 🟪 Organisation
- 🟩 Social media profiles
- 🟩 IT infrastructure
- 🟧 Email addresses
- 🟥 Social media risk
- 🟦 Confidential material
- 🟦 User names

Source: Digital Shadows © Digital Shadows 2012 (www.digitalshadows.com)

Shadow management


Content removal and drown-out

Technology re-configuration

Forensic and legal investigation

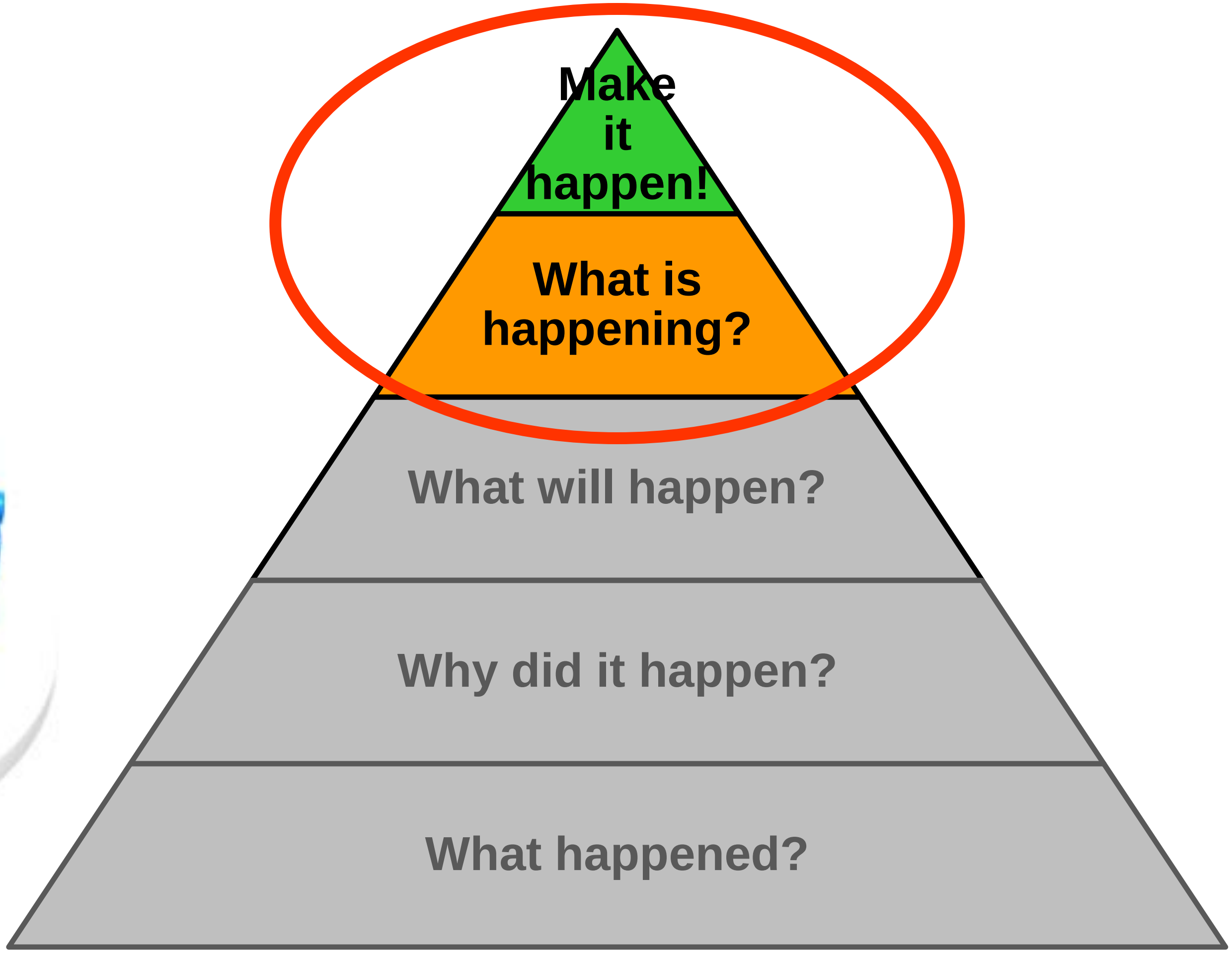
Social media policy and compliance

Training and testing

Resilient Thinking

Source: Digital Shadows © Digital Shadows 2012 www.digitalshadows.com

Exploiting other shadows (broadcasts)



Make it happen!

What is happening?

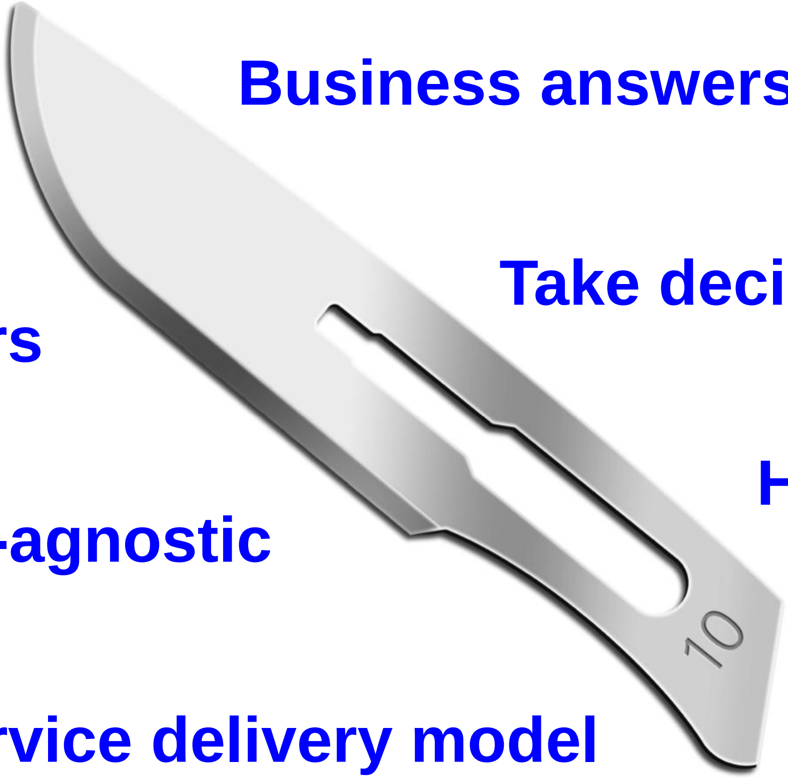
What will happen?

Why did it happen?

What happened?

A new intelligence philosophy

"If I only have finite resources then where should I apply them in order to achieve my business goals?"



Business answers

Take decisions

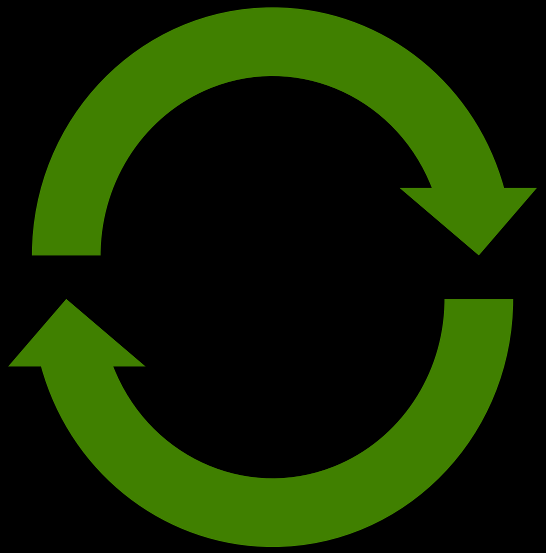
No sledgehammers

Hide complexity

IT-agnostic

Service delivery model

Getting the answers

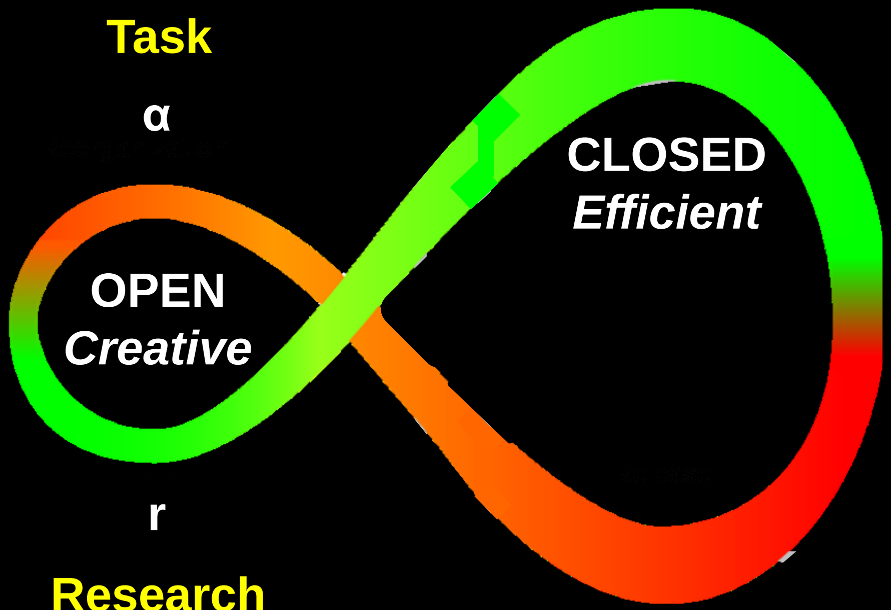


Task

Research

Refinement

Investigation



Investigation

K

Task

α

CLOSED

Efficient

OPEN

Creative

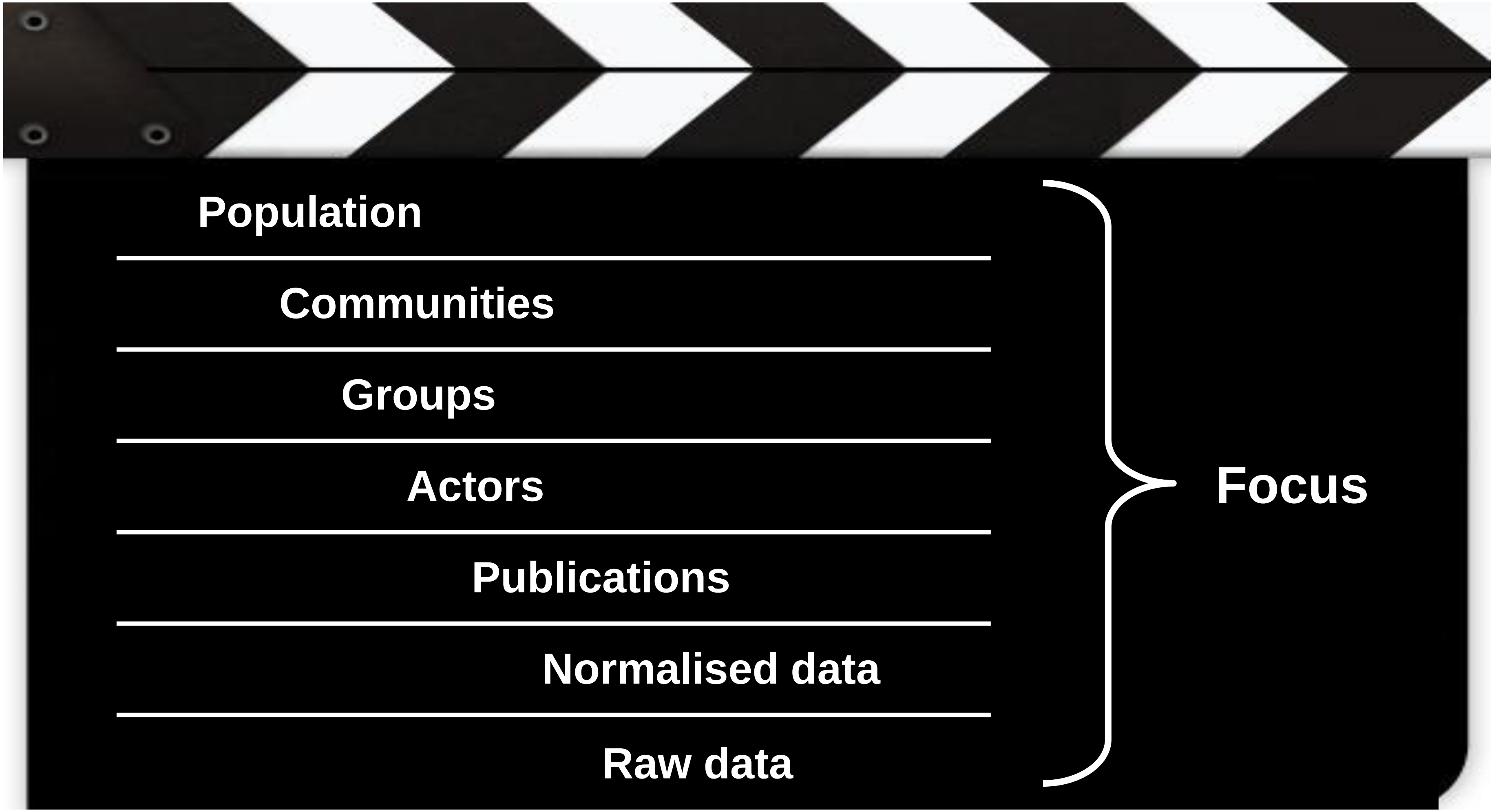
r

Research

Ω

Refinement

Social analysis model



Population

Communities

Groups

Actors

Publications

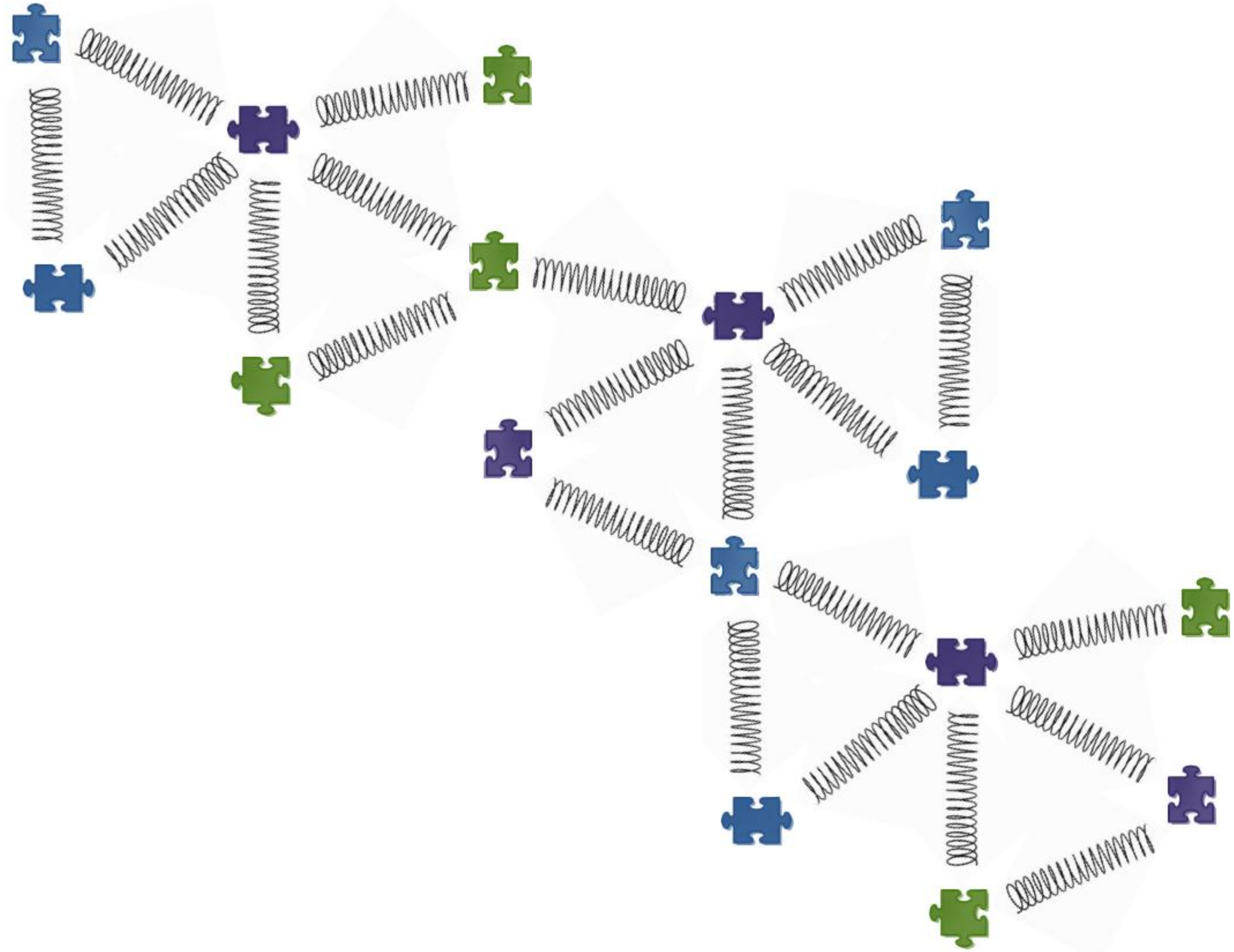
Normalised data

Raw data

Focus

Source: Primary Key Associates © Primary Key Associates 2012 (www.primarykey.co.uk)

Visualisation: traditional approach

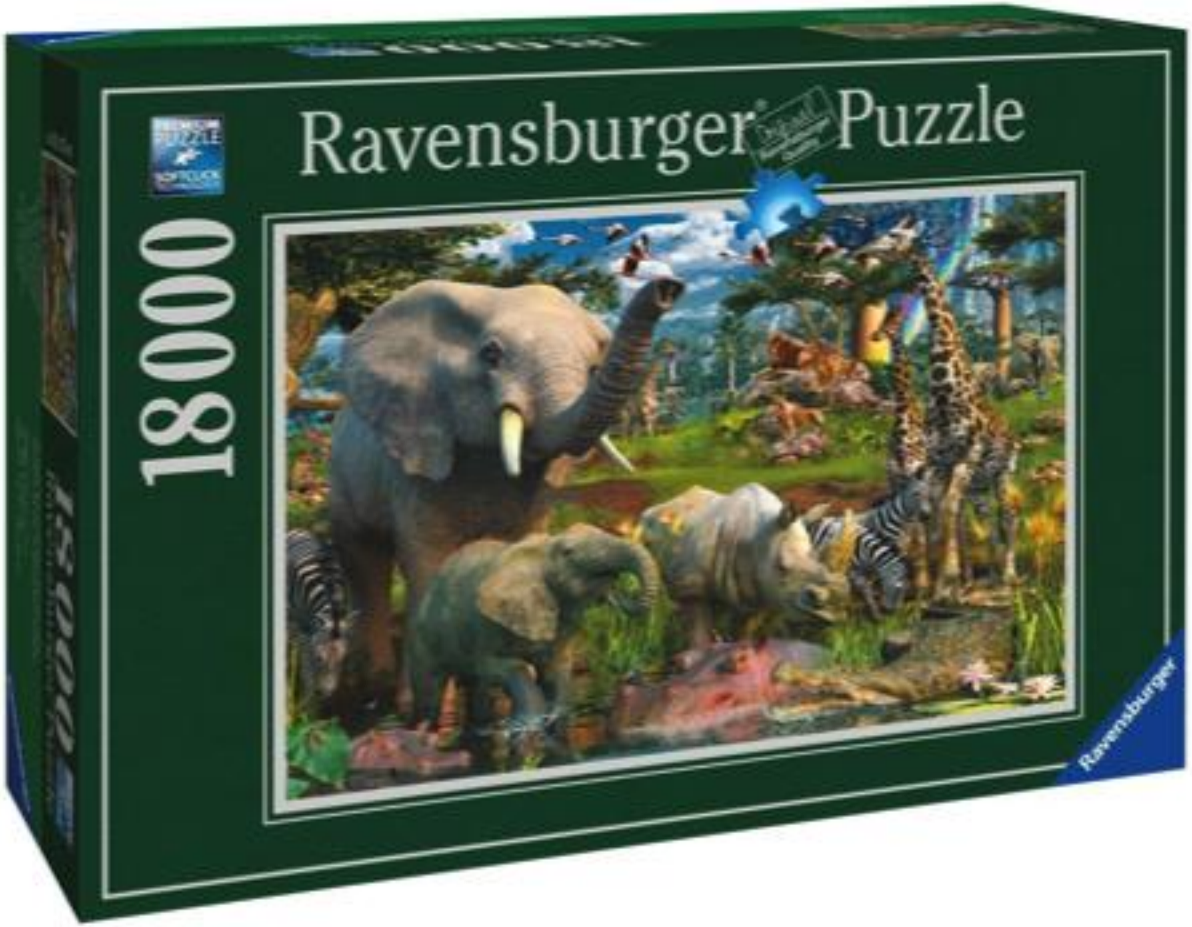


Complex

Non-integrated

“Questions”

Visualisation: alternative approach

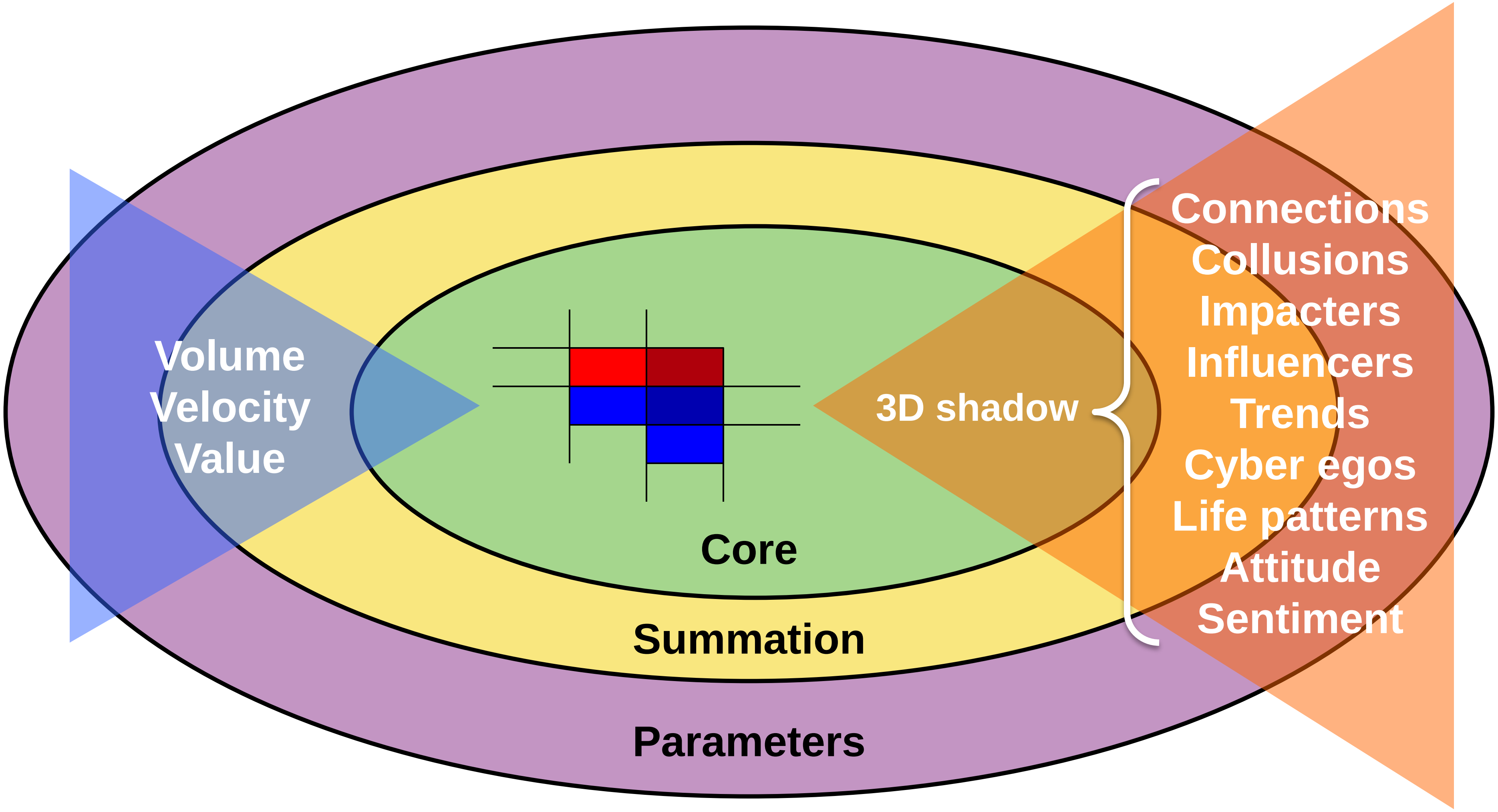


Simple

Integrated

“Answers”

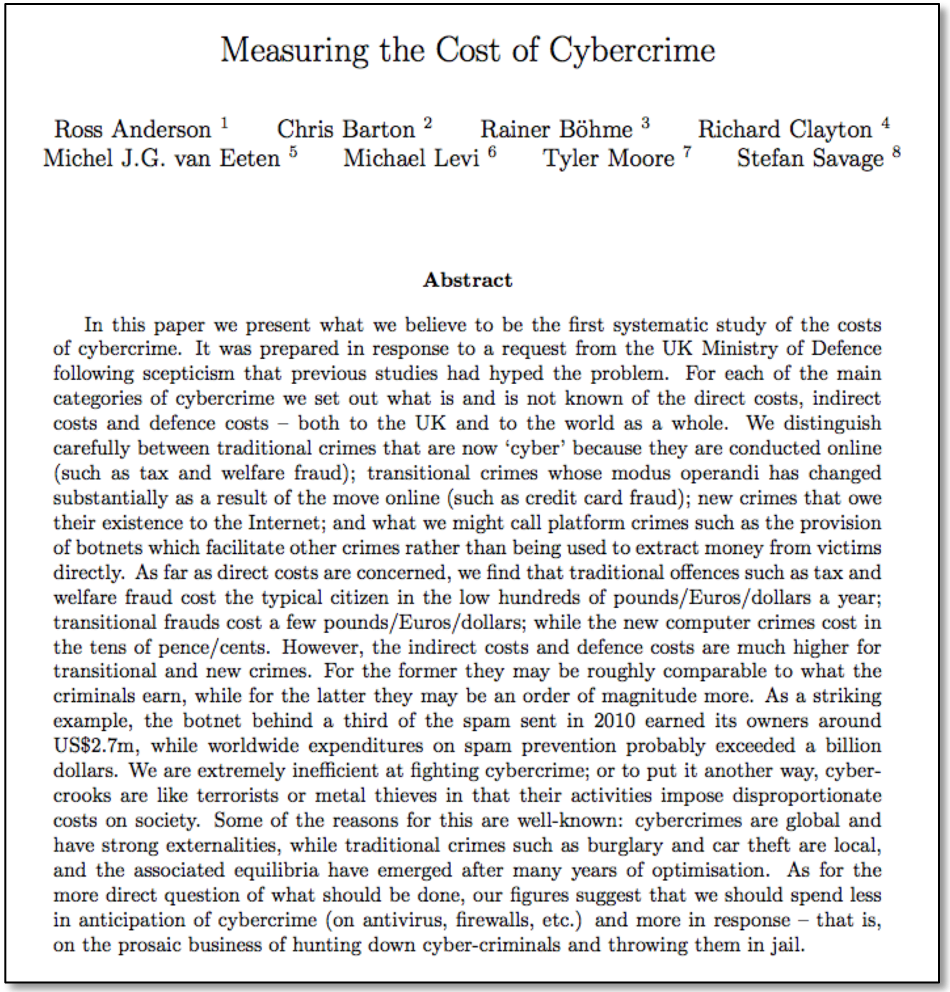
Visualisation: delivering real intelligence



Resilient Thinking

Source: Primary Key Associates © Primary Key Associates 2012 (www.primarykey.co.uk)

Engaging with the threat



Measuring the Cost of Cybercrime

Ross Anderson[1] Chris Barton[2] Rainer Böhme[3] Richard Clayton[4]
Michel J.G. van Eeten[5] Michael Levi[6] Tyler Moore[7] Stefan Savage[8]

Abstract

In this paper we present what we believe to be the first systematic study of the costs of cybercrime. It was prepared in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem. For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole. We distinguish carefully between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly. As far as direct costs are concerned, we find that traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/Euros/dollars a year; transitional frauds cost a few pounds/Euros/dollars; while the new computer crimes cost in the tens of pence/cents. However, the indirect costs and defence costs are much higher for transitional and new crimes. For the former they may be roughly comparable to what the criminals earn, while for the latter they may be an order of magnitude more. As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society. Some of the reasons for this are well-known: cybercrimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local, and the associated equilibria have emerged after many years of optimisation. As for the more direct question of what should be done, our figures suggest that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.

"…we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc) and more in response — that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail"

Measuring the cost of cybercrime
Ross Anderson et al
University of Cambridge, 2012

A mightier sword?

Potential benefits

Shadow management

Reduce attackable surface
Protect confidential data
Protect reputation
Ensure compliance

Shadow exploitation

Evidential data gathering
Topic-based analysis
Answers delivered daily
Take tactical/strategic decisions

Where will this take us?

HT207: “Cyber crime, easy as pie and damn ingenious”

HT-108: “How to rob an online bank and get away with it”

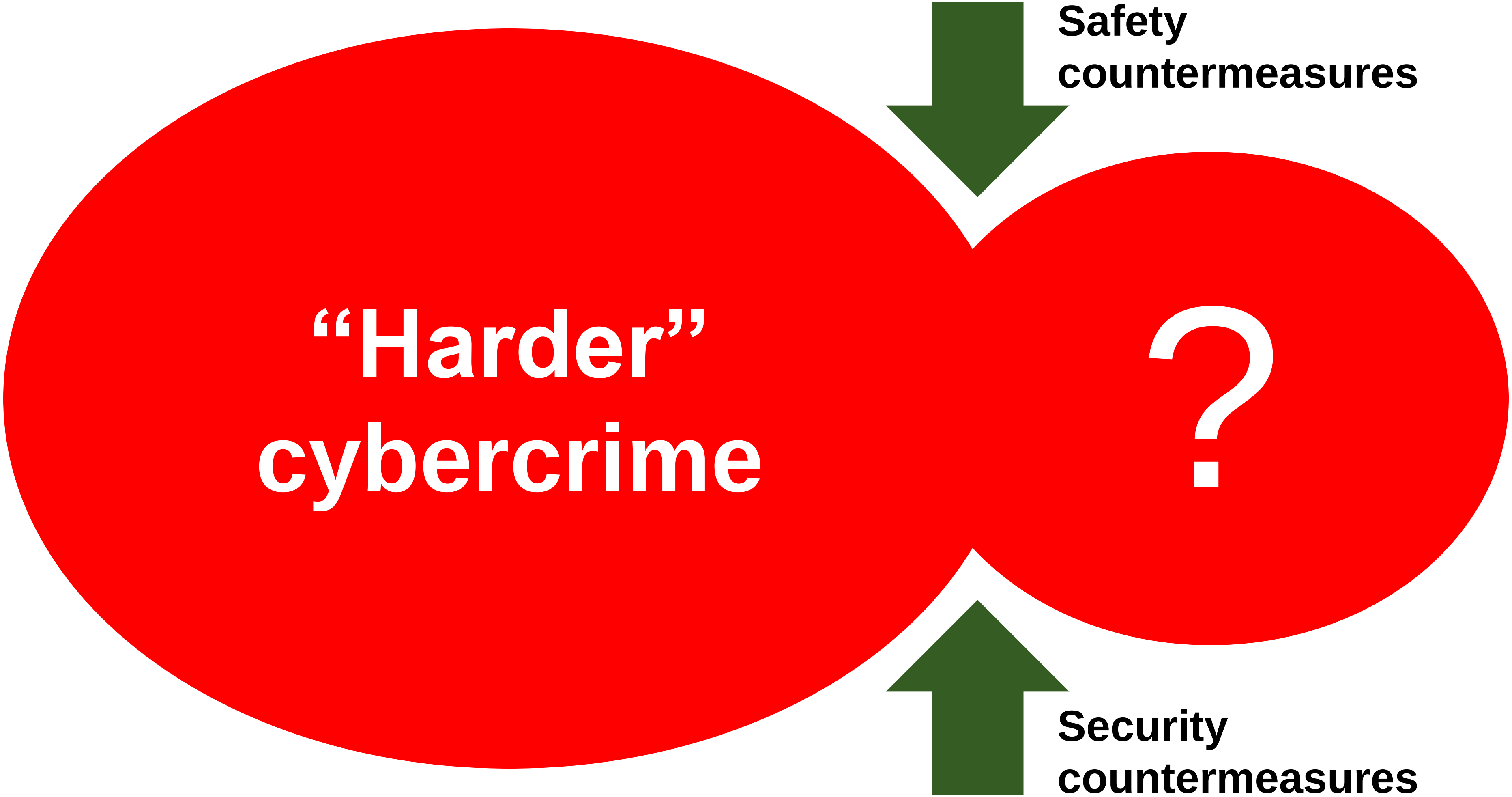
“Easy” cybercrime

4.2m infosec workers by 2015 (13.2% CAGR)

Resilient Thinking

Source: Global Information Security Workforce Study, Frost & Sullivan/(ISC)², 2011

Putting the squeeze on cybercrime



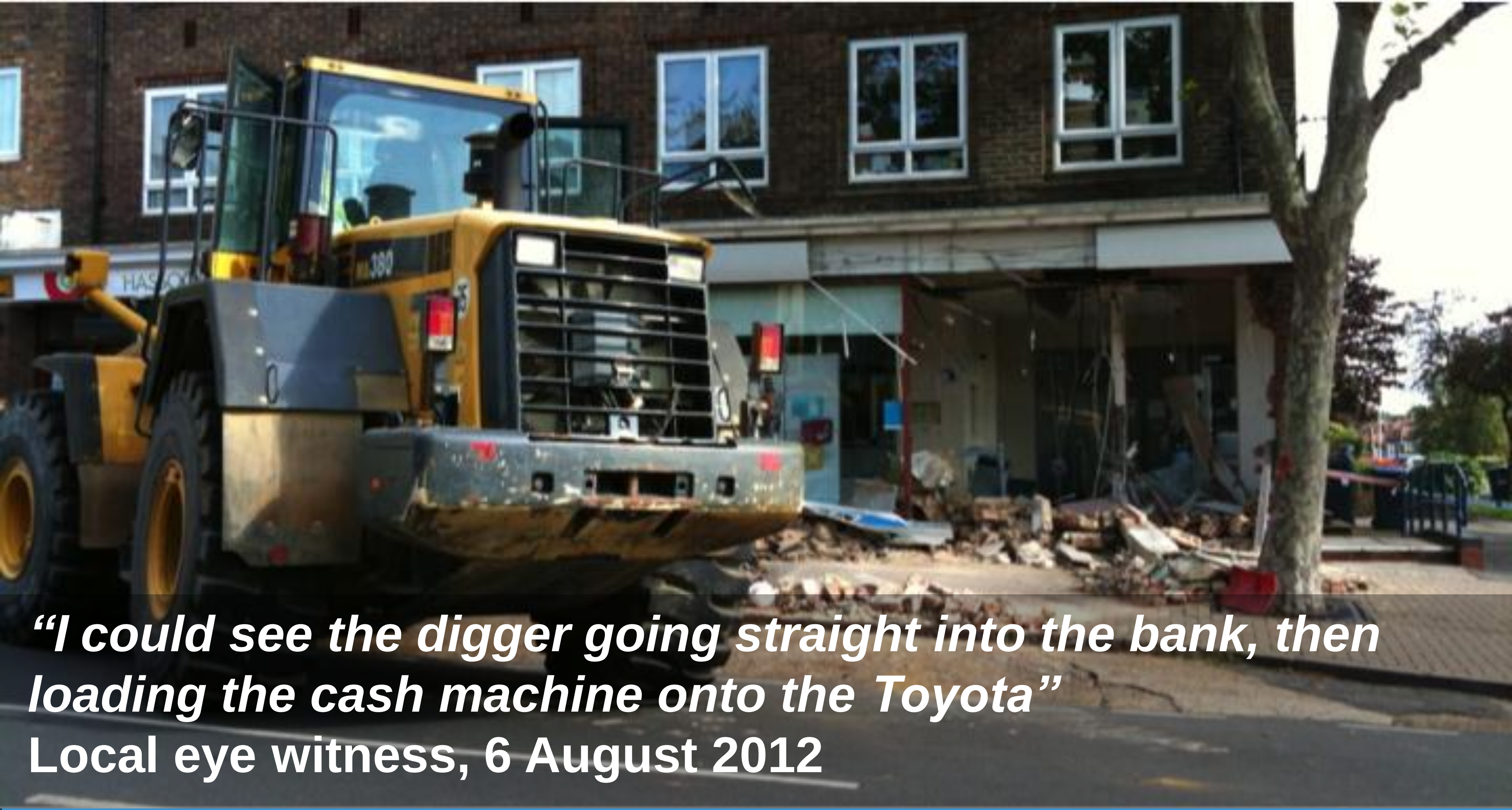
Safety countermeasures

"Harder" cybercrime

?

Security countermeasures

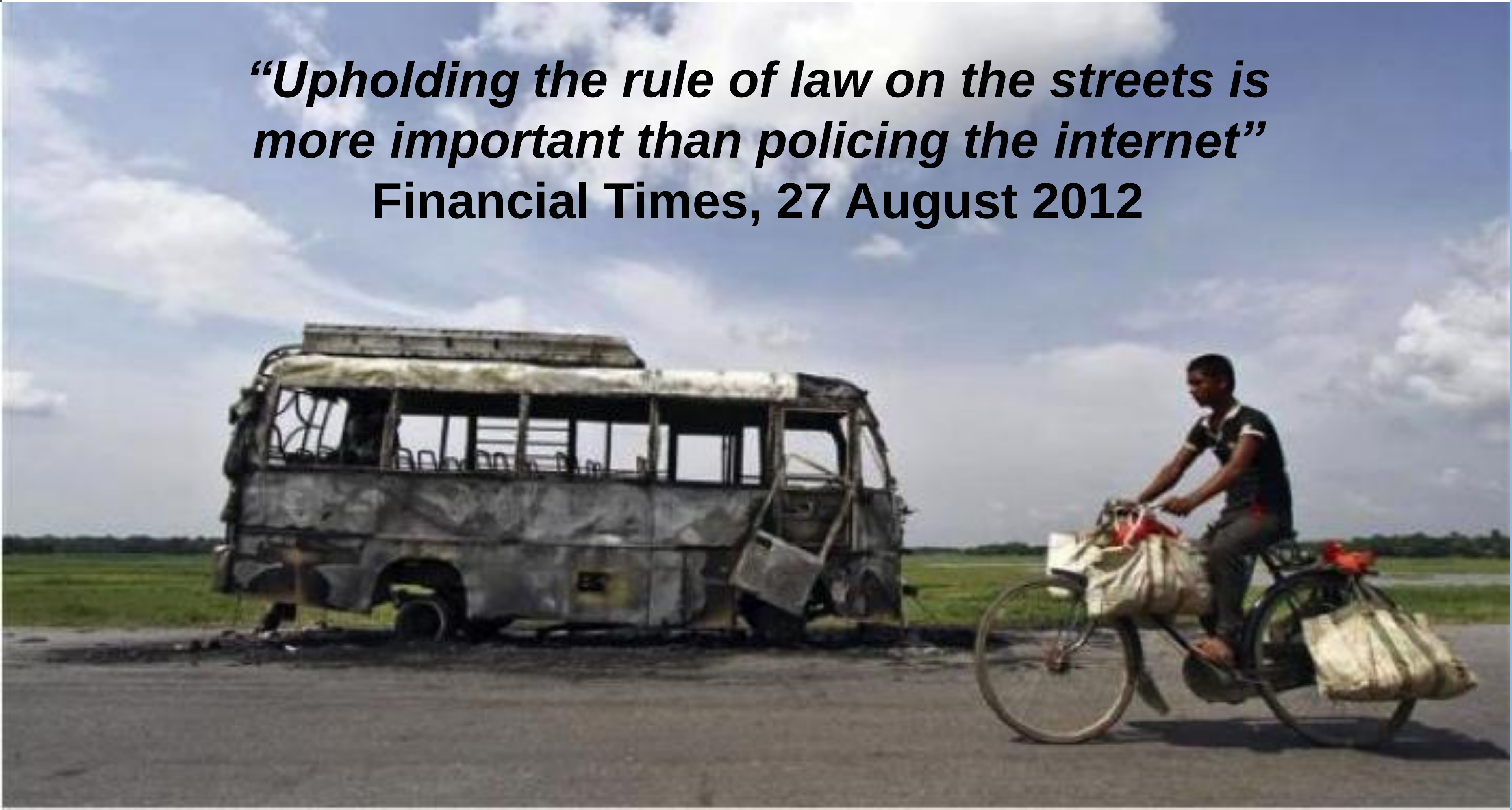
Smash-and-grab: Hassocks, England



"I could see the digger going straight into the bank, then loading the cash machine onto the Toyota"

Local eye witness, 6 August 2012

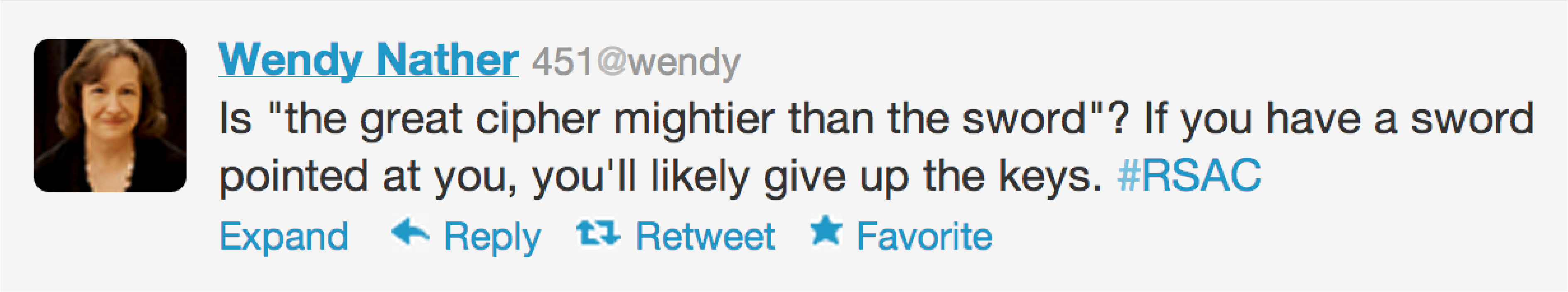
Violence and censorship: Assam, India



"Upholding the rule of law on the streets is more important than policing the internet"

Financial Times, 27 August 2012

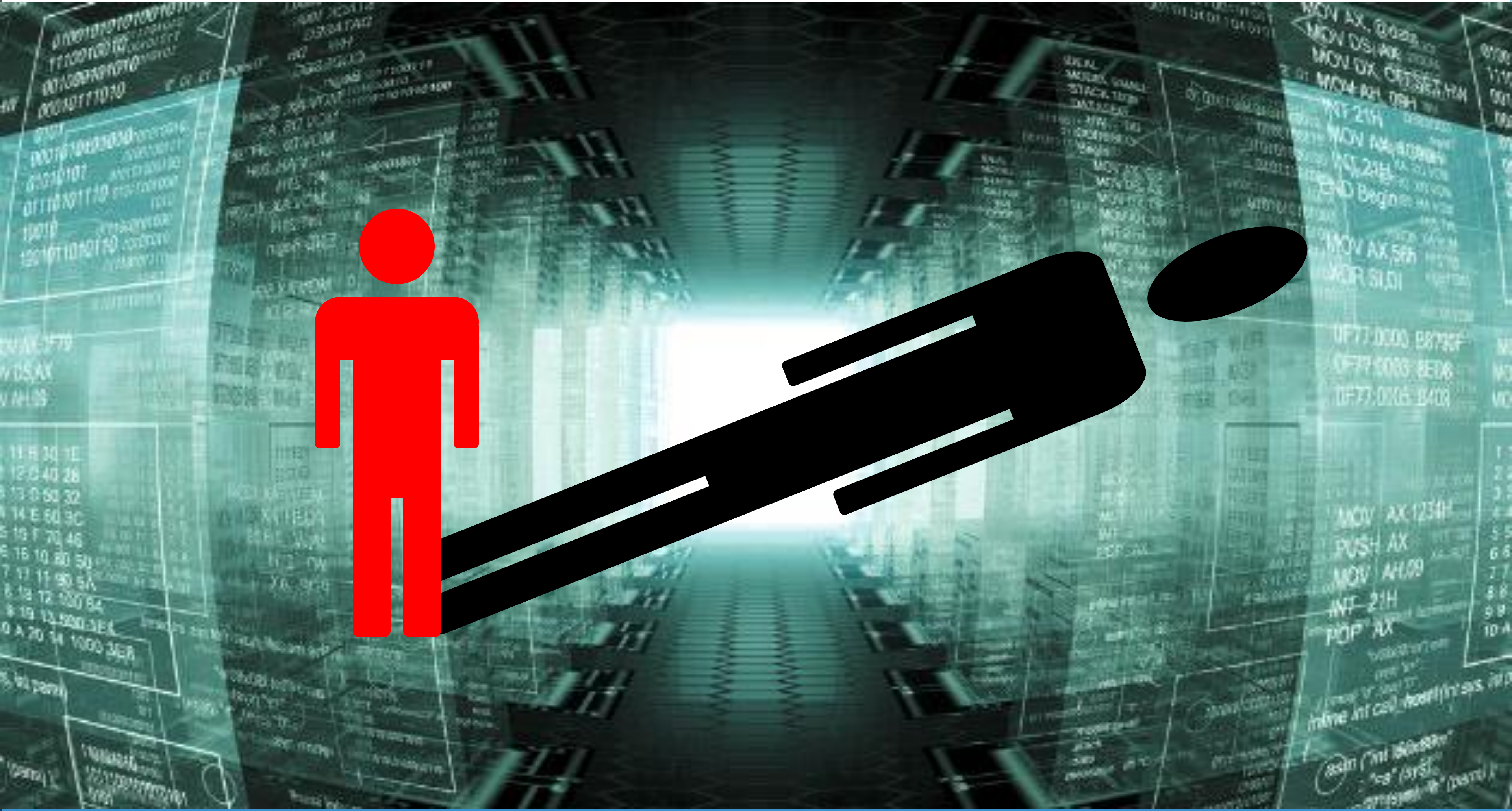
RSA Europe Day 1 conference tweet



Wendy Nather 451@wendy

Is "the great cipher mightier than the sword"? If you have a sword pointed at you, you'll likely give up the keys. #RSAC

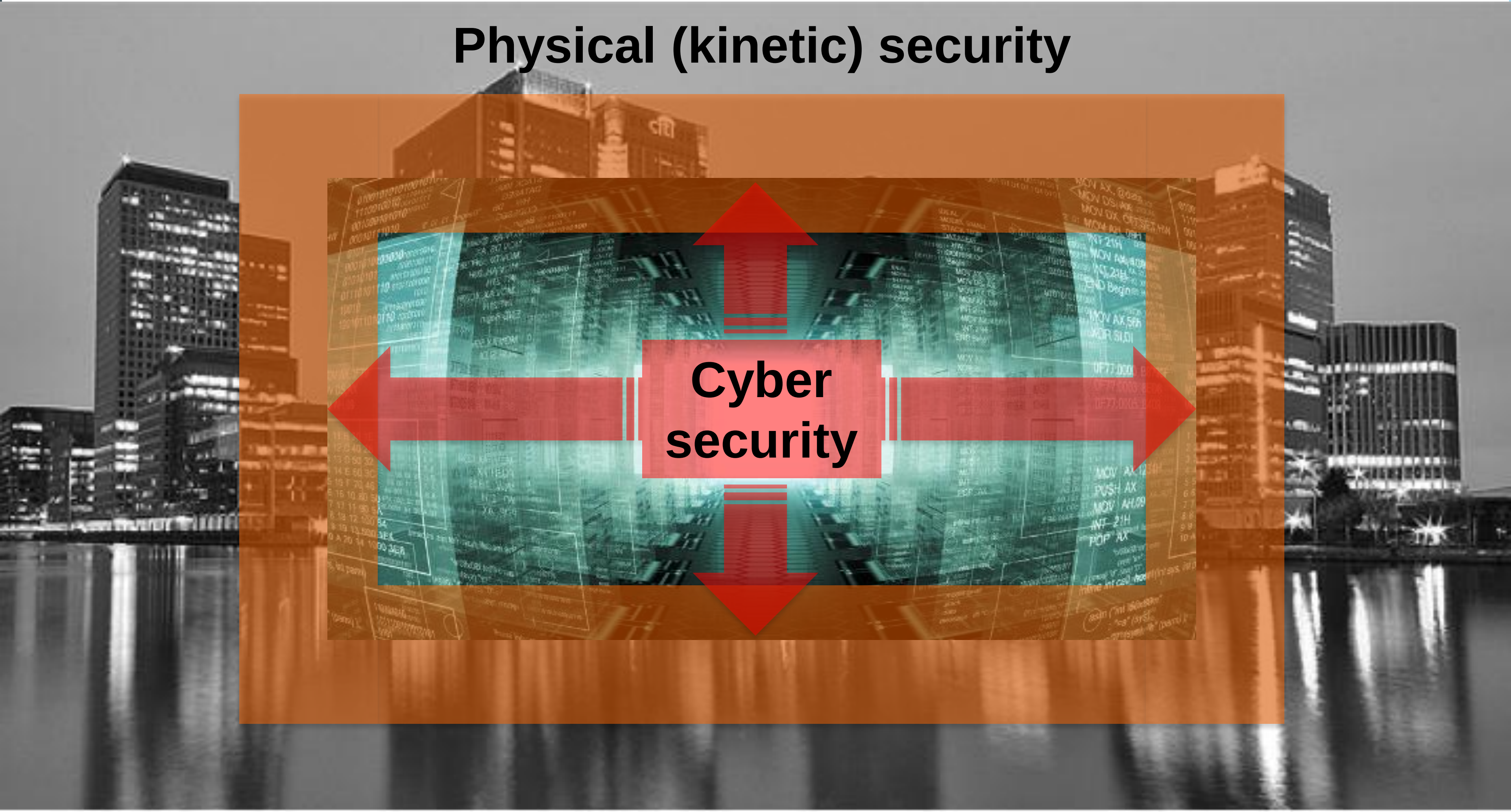
The reality: we live in a physical world



The reality: we live in a physical world

Photo courtesy of Arpad Lukacs, "Canary Wharf Reflections", http://arpadlukacs.com/

A shift in focus: cyber goes kinetic



Cyberkinetic security: culture clash

The Tallinn Manual on the International Law Applicable to Cyber Warfare
NATO Cooperative Cyber Defence Centre of Excellence, 2013

Apply

Applying today's lessons

1. Are you <u>certain</u> you know what "risk" means?

Register as a trial user with an online dependency modelling tool

Develop a first-cut "broad-to-narrow" model that focuses on a key subset of your operations

Compare against your current risk register and review findings with Risk

Applying today’s lessons

2. Is your organisation's digital shadow under control?

Review your employee online activity policy — especially social web publishing

Assess your ability to reduce your attackable surface and remove — or “drown out” — sensitive information that has gone public

Review your findings with HR and Risk

Applying today's lessons

3. Are you getting <u>true intelligence</u> from published social web data?

Review your current data analytics facility — can it analyse social web data and can it scale upwards?

Assess your ability to find threats to your business from an "outside looking in" analytical perspective

Review findings with Risk and/or Marketing

Thank you – any questions?

david.porter@resilientthinking.co.uk

www.resilientthinking.co.uk