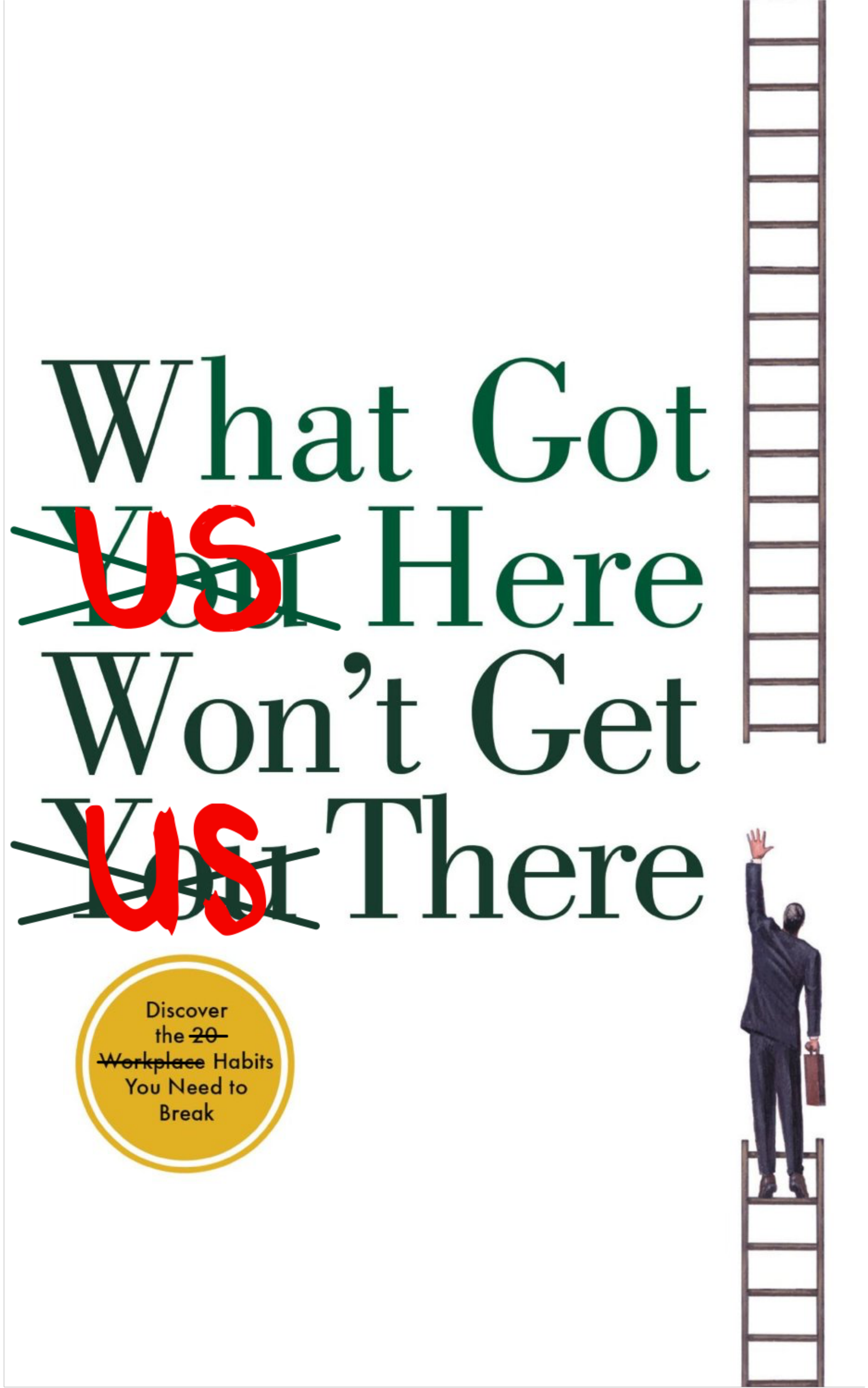


What Got ~~You~~ us Here Won't Get ~~You~~ us There

Discover the ~~20~~ ~~Workplace~~ Habits You Need to Break

@haroonmeer
Thinkst

THANKS!

thinkst
applied research

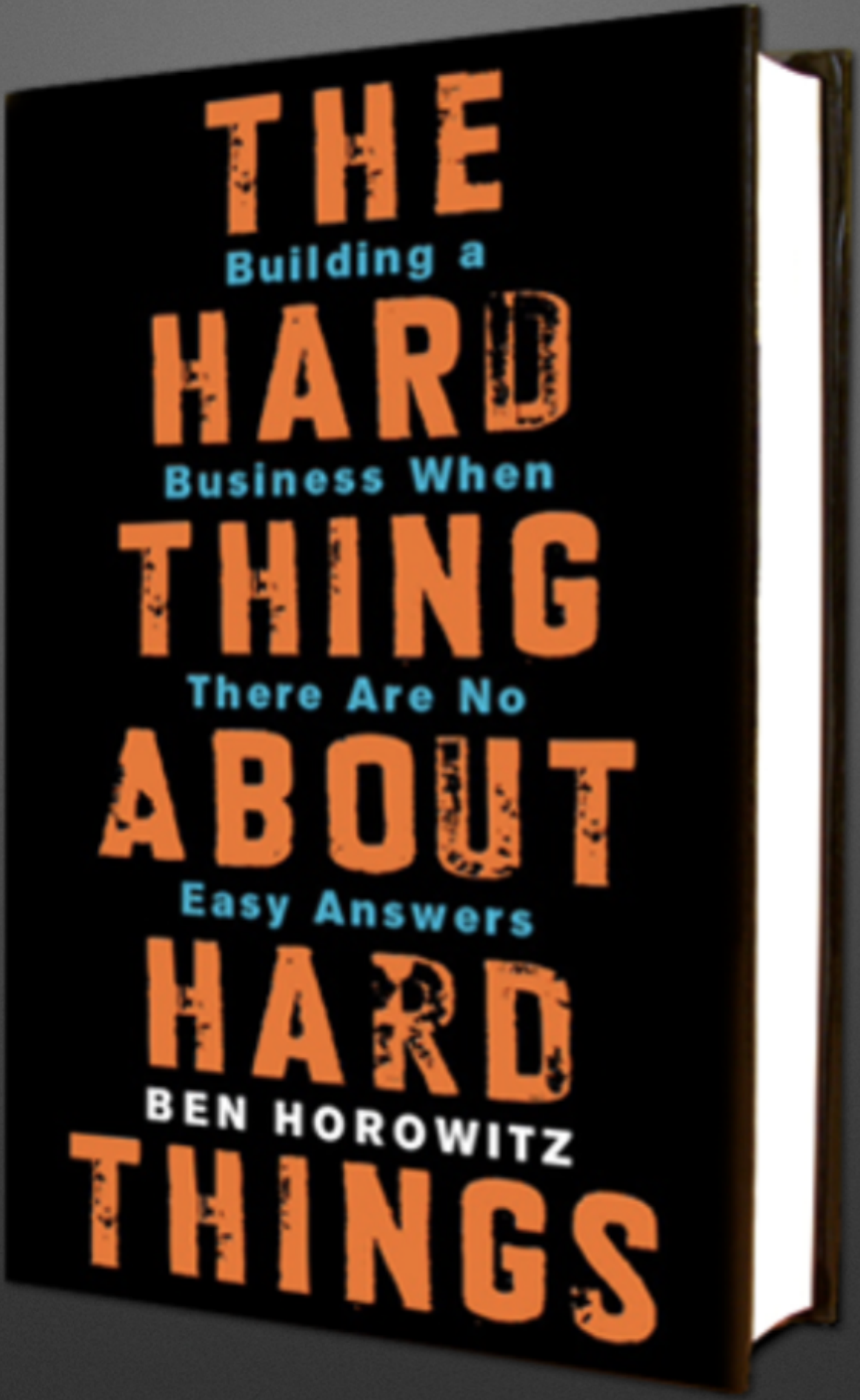
haroon meer

@haroonmeer

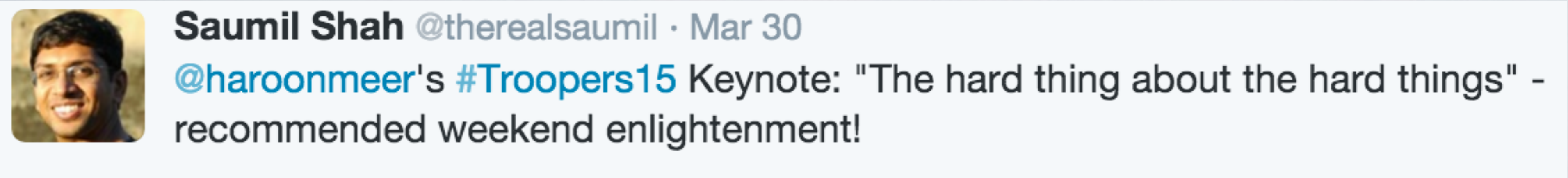
thinkst
applied research

Whats with the cheesy title?

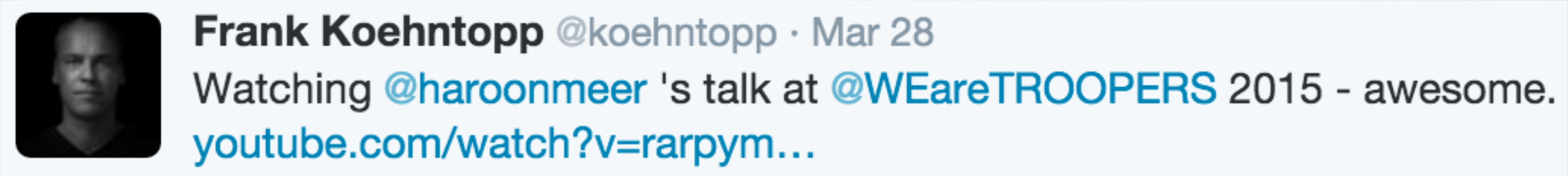
https://www.youtube.com/watch?v=rarpym8JJXQ



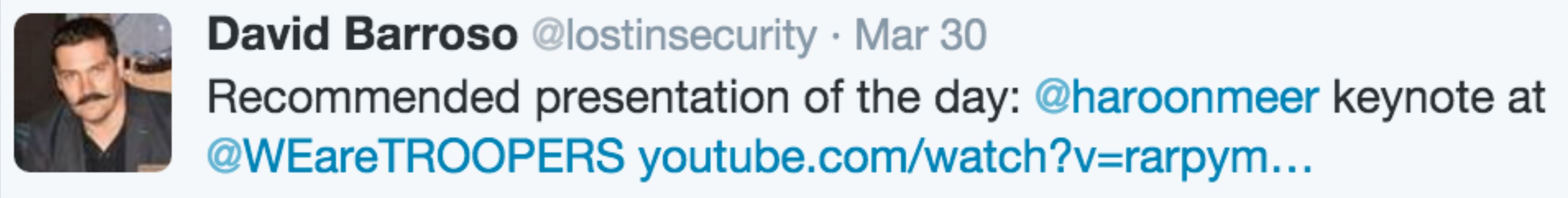
thinkst
applied research


Saumil Shah @therealsaumil · Mar 30

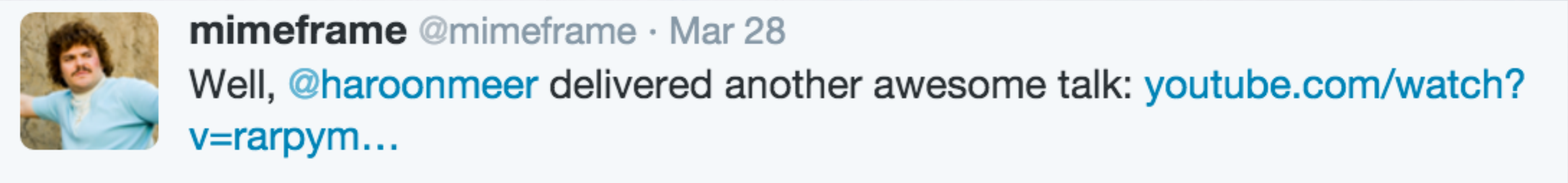
@haroonmeer's #Troopers15 Keynote: "The hard thing about the hard things" - recommended weekend enlightenment!


Frank Koehntopp @koehntopp · Mar 28

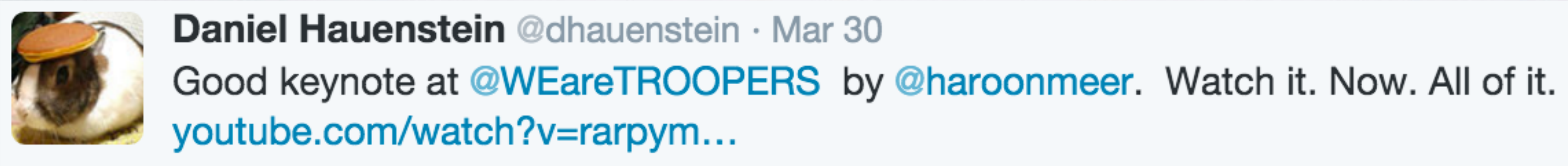
Watching @haroonmeer 's talk at @WEareTROOPERS 2015 - awesome. youtube.com/watch?v=rarpym…


David Barroso @lostinsecurity · Mar 30

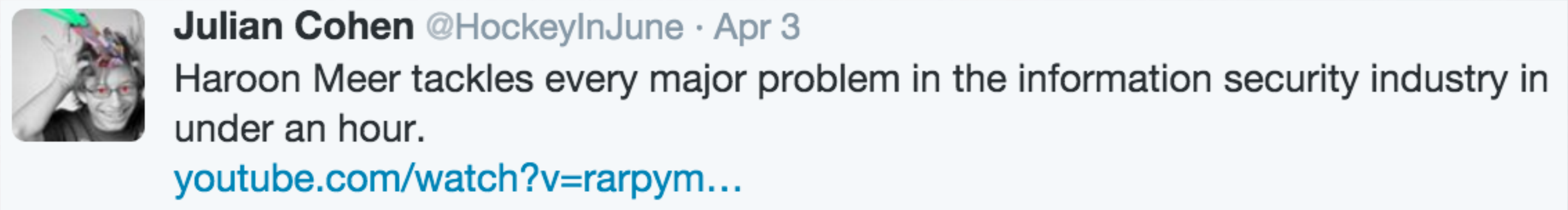
Recommended presentation of the day: @haroonmeer keynote at @WEareTROOPERS youtube.com/watch?v=rarpym…


mimeframe @mimeframe · Mar 28

Well, @haroonmeer delivered another awesome talk: youtube.com/watch?v=rarpym…

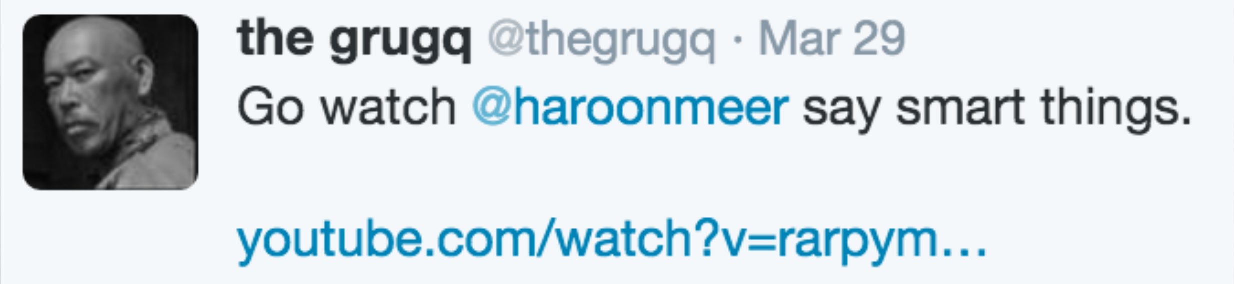

Daniel Hauenstein @dhauenstein · Mar 30

Good keynote at @WEareTROOPERS by @haroonmeer. Watch it. Now. All of it. youtube.com/watch?v=rarpym…


Julian Cohen @HockeyInJune · Apr 3

Haroon Meer tackles every major problem in the information security industry in under an hour.

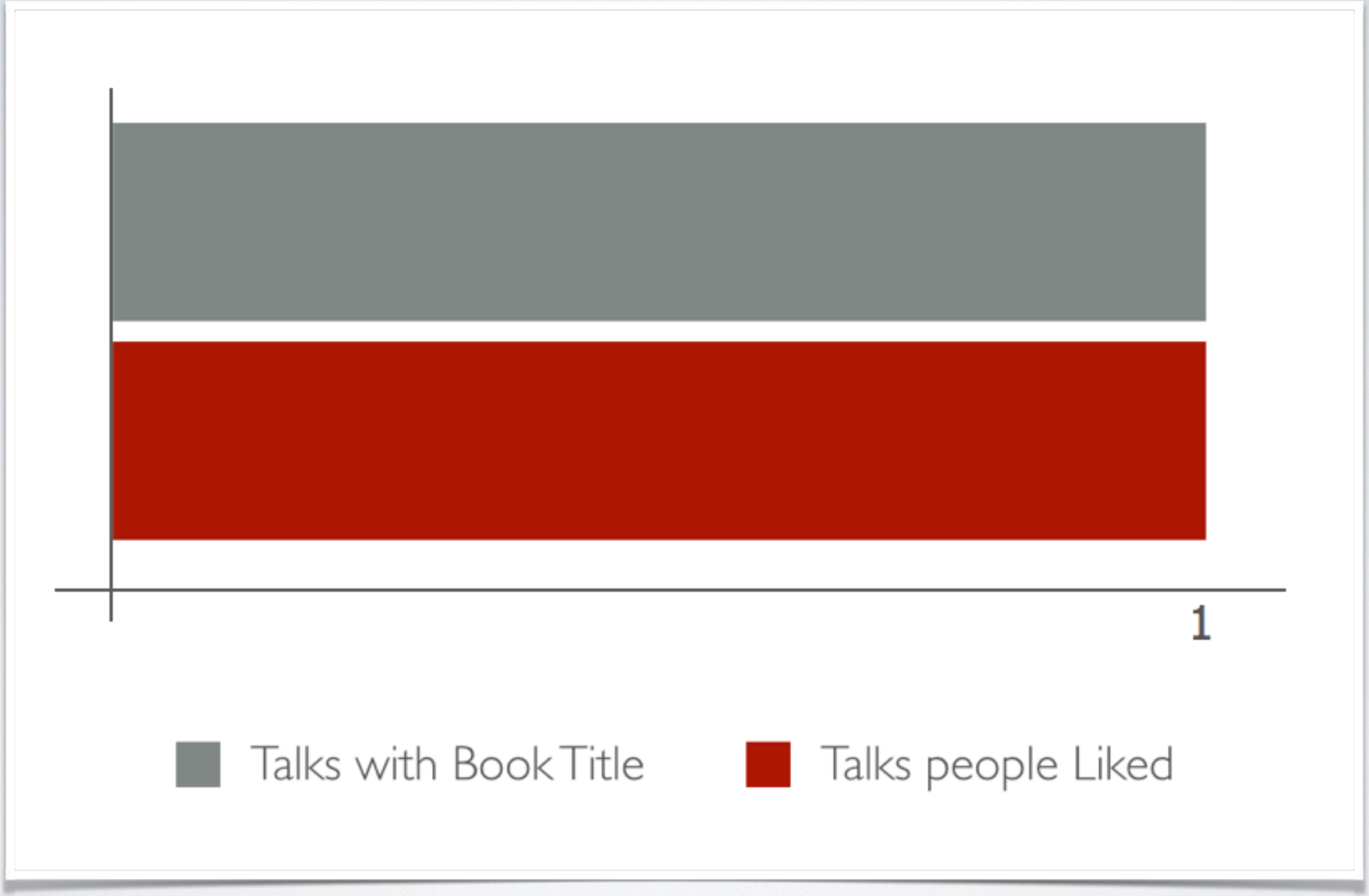
youtube.com/watch?v=rarpym…


the grugq @thegrugq · Mar 29

Go watch @haroonmeer say smart things.

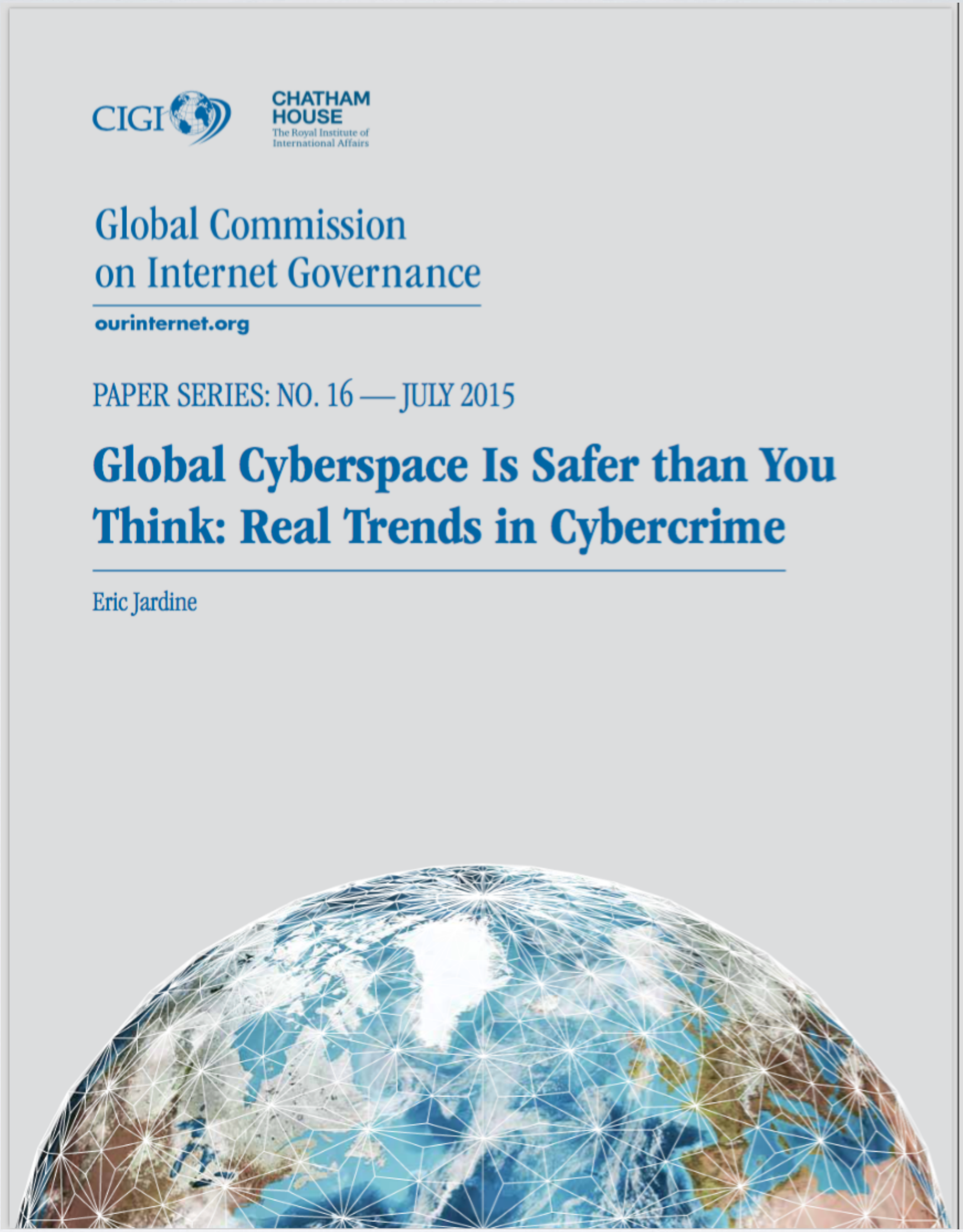
youtube.com/watch?v=rarpym…

thinkst
applied research


1
Talks with Book Title
Talks people Liked

but.. before we go on

Is this even a problem?



CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

Global Commission
on Internet Governance

ourinternet.org

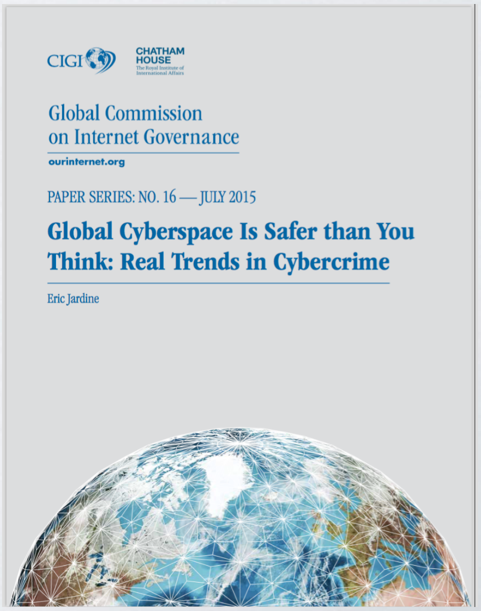
PAPER SERIES: NO. 16 — JULY 2015

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime

Eric Jardine

https://www.cigionline.org/sites/default/files/no16_web_1.pdf

"This paper argues that the level of security in cyberspace is actually far better than the picture described by media accounts and IT security reports."



CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission
on Internet Governance

ourinternet.org

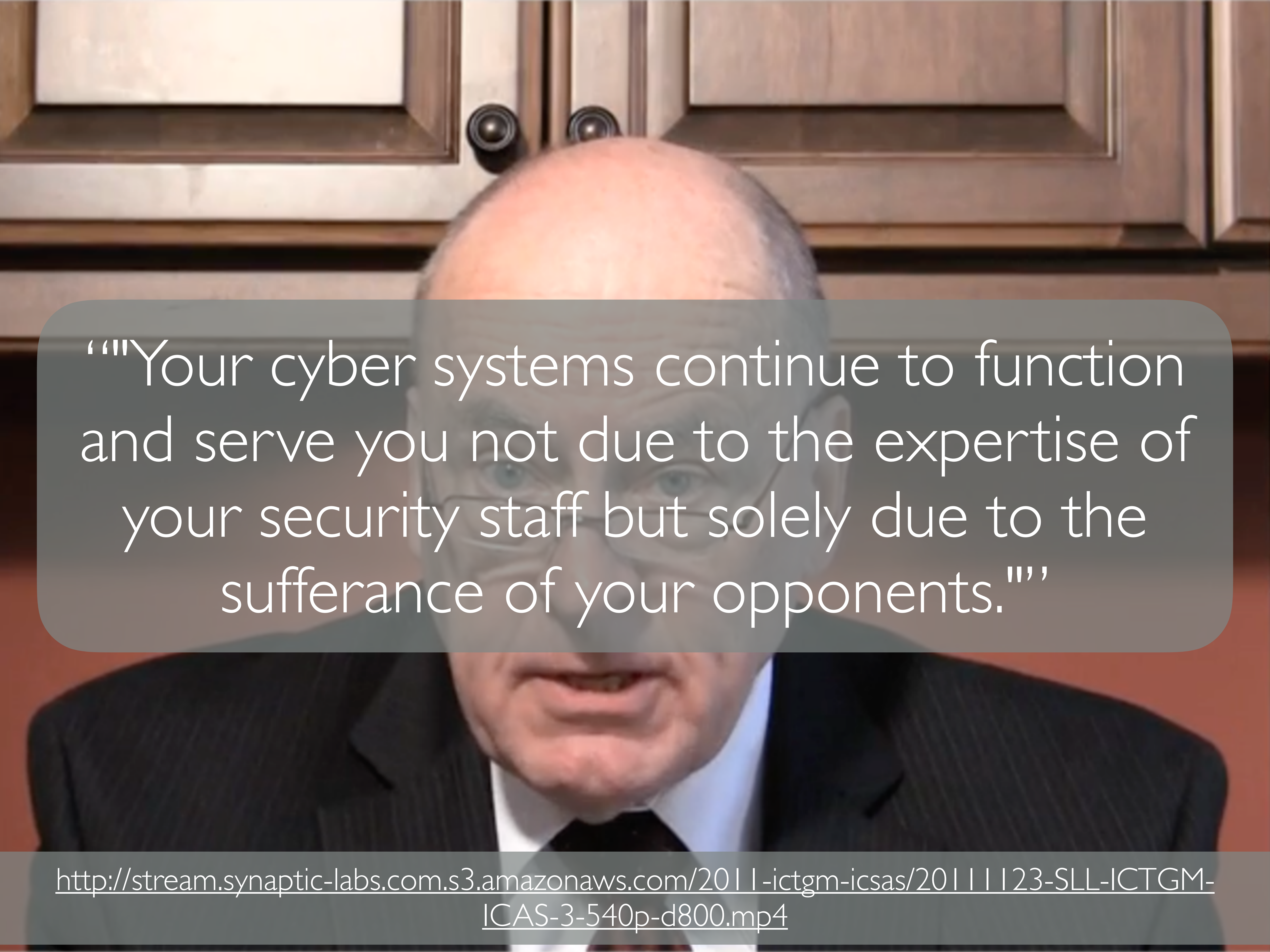
PAPER SERIES: NO. 16 — JULY 2015

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime

Eric Jardine

https://www.cigionline.org/sites/default/files/no16_web_1.pdf

"Our Cyber Security Status is Grim (and the way ahead will be hard)"



‘“"Your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents."”’

http://stream.synaptic-labs.com.s3.amazonaws.com/2011-ictgm-icsas/20111123-SLL-ICTGM-ICAS-3-540p-d800.mp4

“Our upcoming security apocalypse”

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

“a crisis of confidence”

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

thinkst
applied research

“‘a simple litmus test’”

thinkst
applied research

"…imagine the highest value individual at your corporation"

“Can you stop a determined attacker from compromising him?”

““how ineffectual can we be?””

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

"For the thousands your organization spends on security, you can't protect the one guy who is most valuable to you. Worse yet, would you even know if he was popped?"

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

‘‘This problem compounds, because the company boards are now increasingly aware of the Infosec problem..’’

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

thinkst
applied research

“‘but they are making the logical assumption that the teams of people they are paying, have the problem under control.’’

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

> “They don't know that we don't have the answers yet, that many of us are resorting to hope as a strategy, hoping desperately that when the breach eventually happens, it won't happen on our watch”

http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html

thinkst
applied research

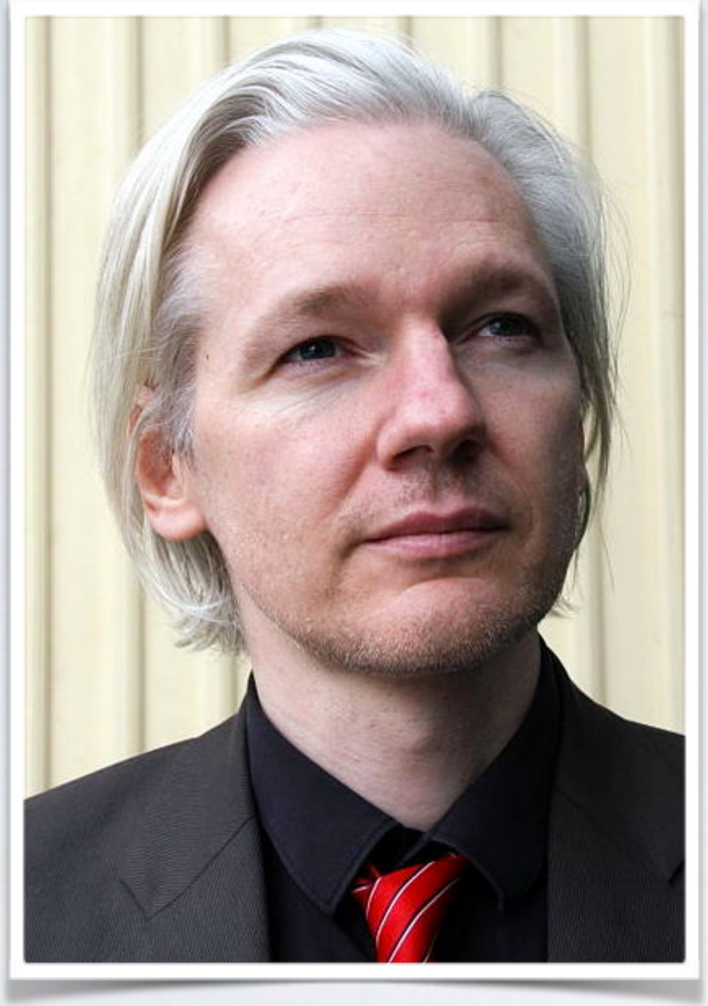
We are already there

“it’s just not evenly distributed yet”

its going to get worse…

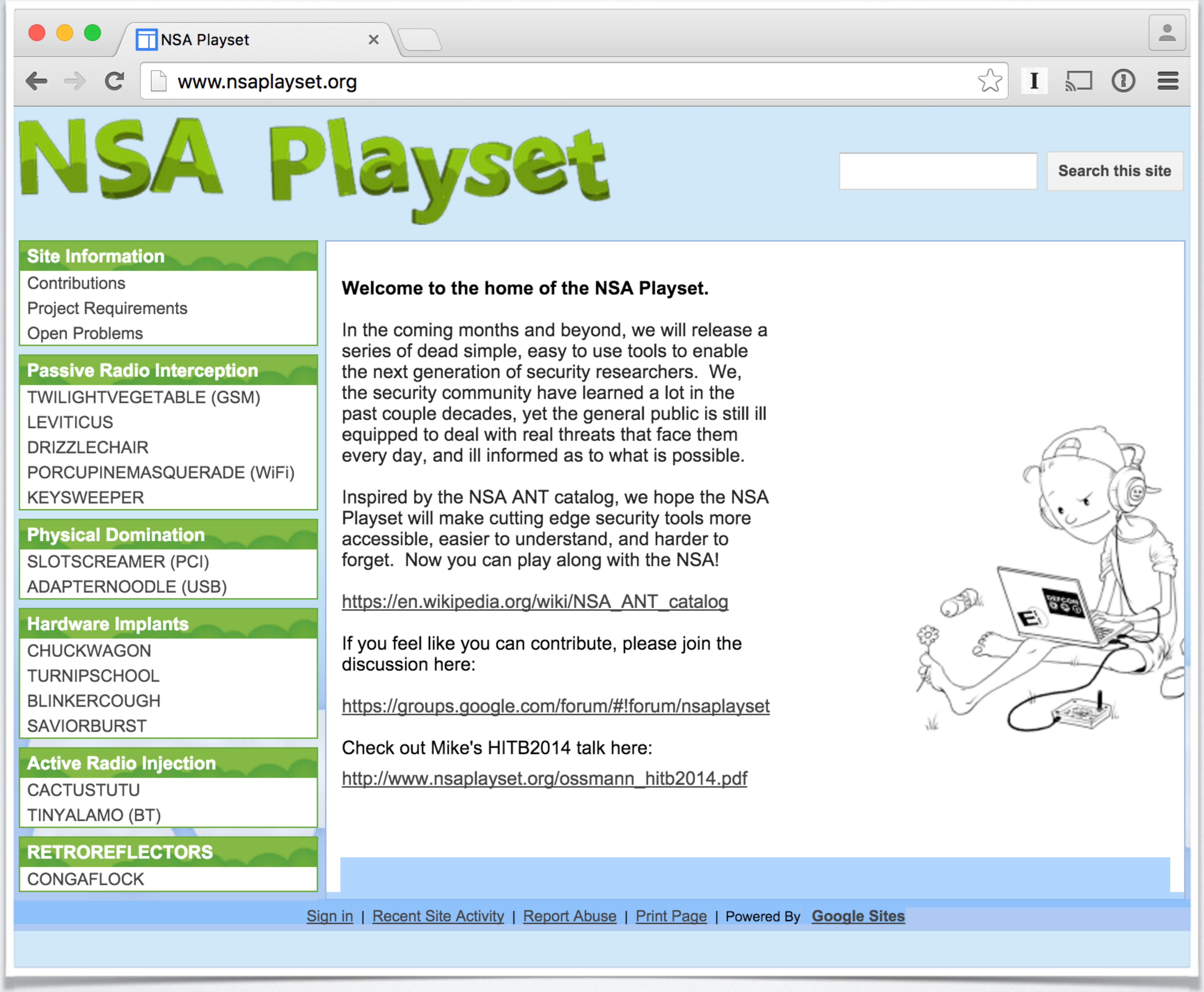
Why?

Why?



“Courage is contagious”

thinkst
applied research


NSA Playset
www.nsaplayset.org
NSA Playset
Search this site
Sign in | Recent Site Activity | Report Abuse | Print Page | Powered By Google Sites

Site Information
- Contributions
- Project Requirements
- Open Problems

Passive Radio Interception
- TWILIGHTVEGETABLE (GSM)
- LEVITICUS
- DRIZZLECHAIR
- PORCUPINEMASQUERADE (WiFi)
- KEYSWEEPER

Physical Domination
- SLOTSCREAMER (PCI)
- ADAPTERNOODLE (USB)

Hardware Implants
- CHUCKWAGON
- TURNIPSCHOOL
- BLINKERCOUGH
- SAVIORBURST

Active Radio Injection
- CACTUSTUTU
- TINYALAMO (BT)

RETROREFLECTORS
- CONGAFLOCK

Welcome to the home of the NSA Playset.

In the coming months and beyond, we will release a series of dead simple, easy to use tools to enable the next generation of security researchers. We, the security community have learned a lot in the past couple decades, yet the general public is still ill equipped to deal with real threats that face them every day, and ill informed as to what is possible.

Inspired by the NSA ANT catalog, we hope the NSA Playset will make cutting edge security tools more accessible, easier to understand, and harder to forget. Now you can play along with the NSA!

https://en.wikipedia.org/wiki/NSA_ANT_catalog

If you feel like you can contribute, please join the discussion here:

https://groups.google.com/forum/#!forum/nsaplayset

Check out Mike's HITB2014 talk here:

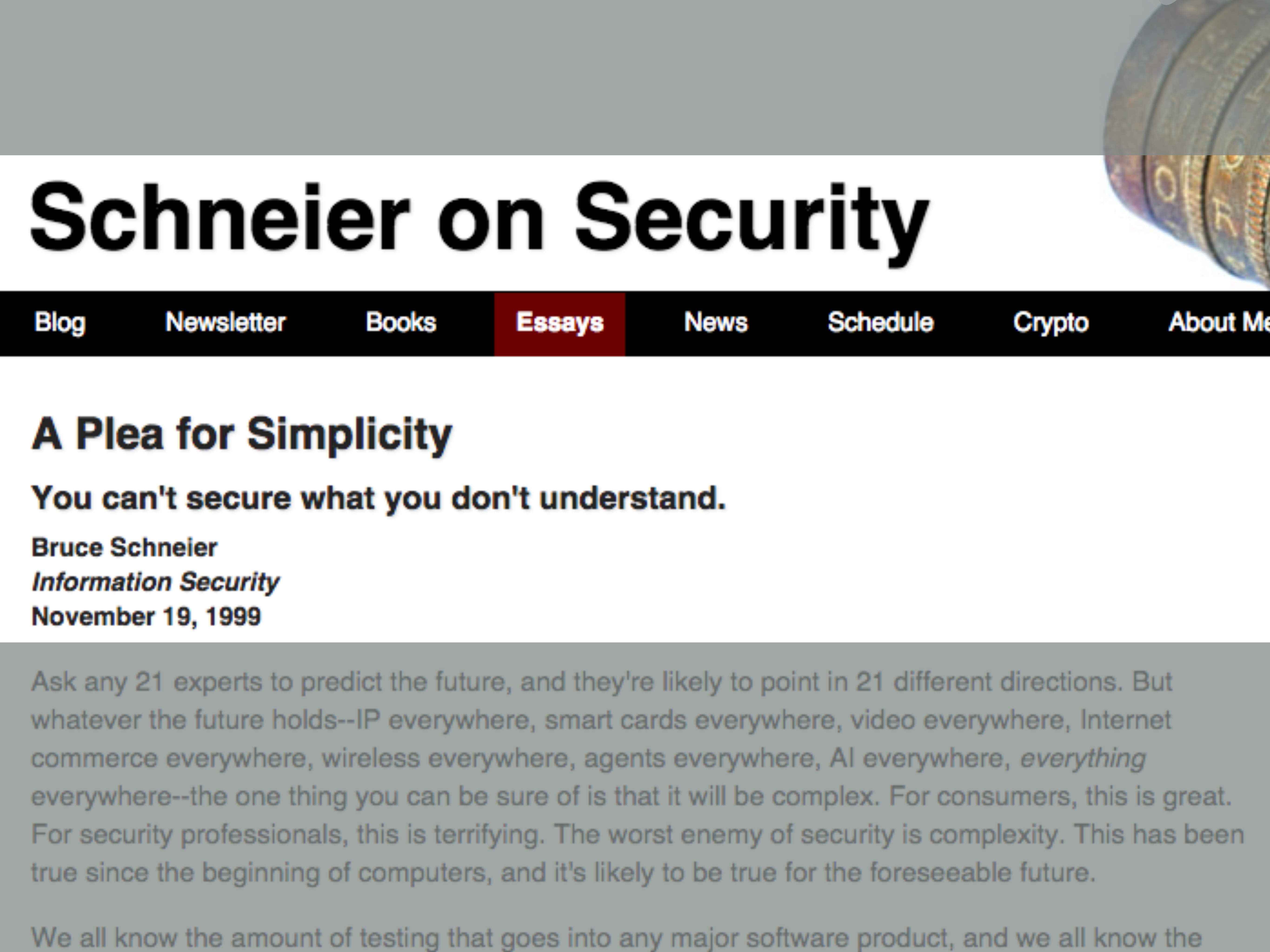
http://www.nsaplayset.org/ossmann_hitb2014.pdf

http://www.nsaplayset.org/

Complexity

https://www.youtube.com/watch?v=rarpym8JJXQ

It’s not a new realisation..



Schneier on Security

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security
November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the epidemic of macro viruses shows that Microsoft Word and Excel need to be secure too. Rogue printer drivers can compromise Windows NT. Malicious attachments can tunnel through firewalls. Maintenance ports on routers can compromise networks, as can random modems. DSL and satellite modems can completely compromise security. So can Java or Microsoft Outlook. Or your recycling bin.

The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.

I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

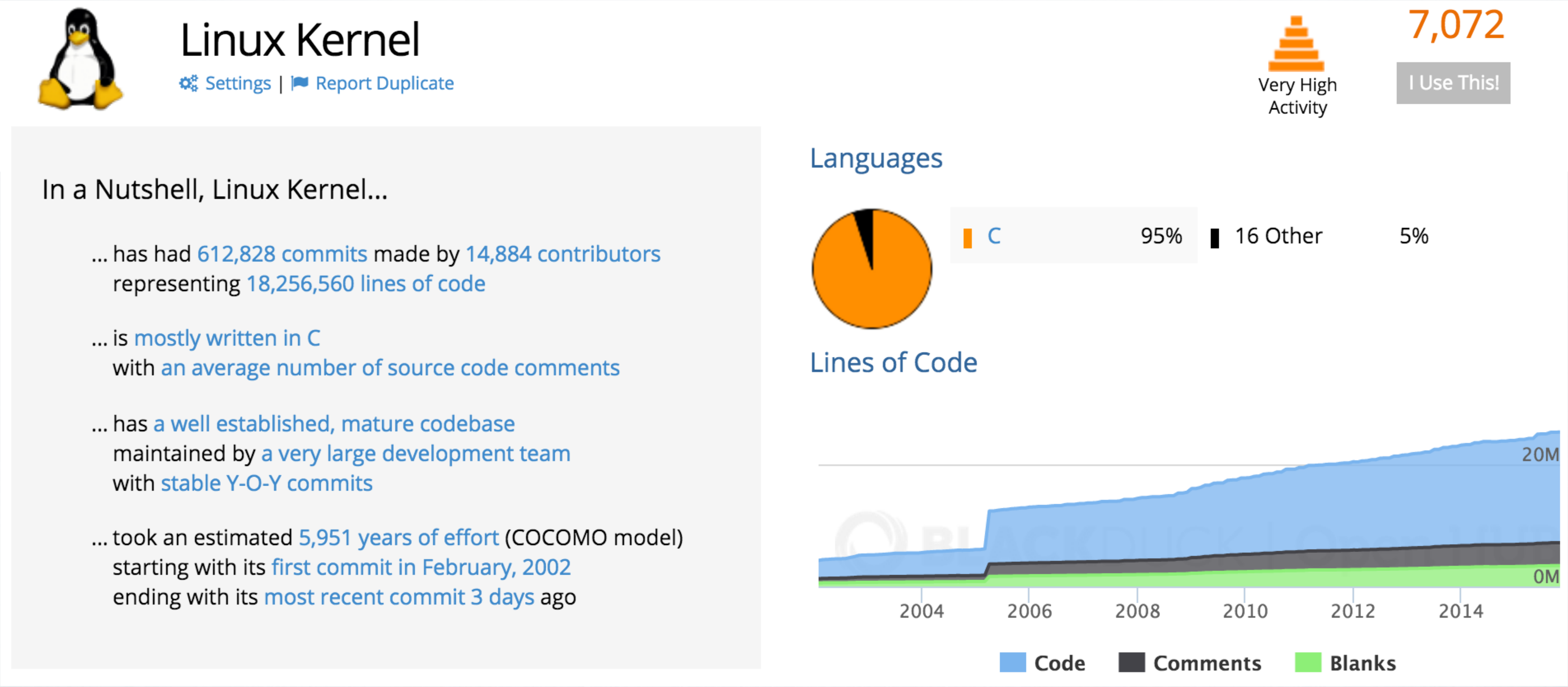
The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.

BRUCE SCHNEIER*is CTO of Counterpane Internet Security Inc., a company trying to bring managed security solutions to complex networks. He writes the CryptoRhythms column for* Information Security, *and is the author of* Applied Cryptography *and the Blowfish and Twofish encryption algorithms.*

Predictions

Linux Kernel (1991)

10,239 (loc)



Linux Kernel

Settings | Report Duplicate

7,072

Very High Activity

I Use This!

In a Nutshell, Linux Kernel...

... has had 612,828 commits made by 14,884 contributors representing 18,256,560 lines of code

... is mostly written in C with an average number of source code comments

... has a well established, mature codebase maintained by a very large development team with stable Y-O-Y commits

... took an estimated 5,951 years of effort (COCOMO model) starting with its first commit in February, 2002 ending with its most recent commit 3 days ago

Languages

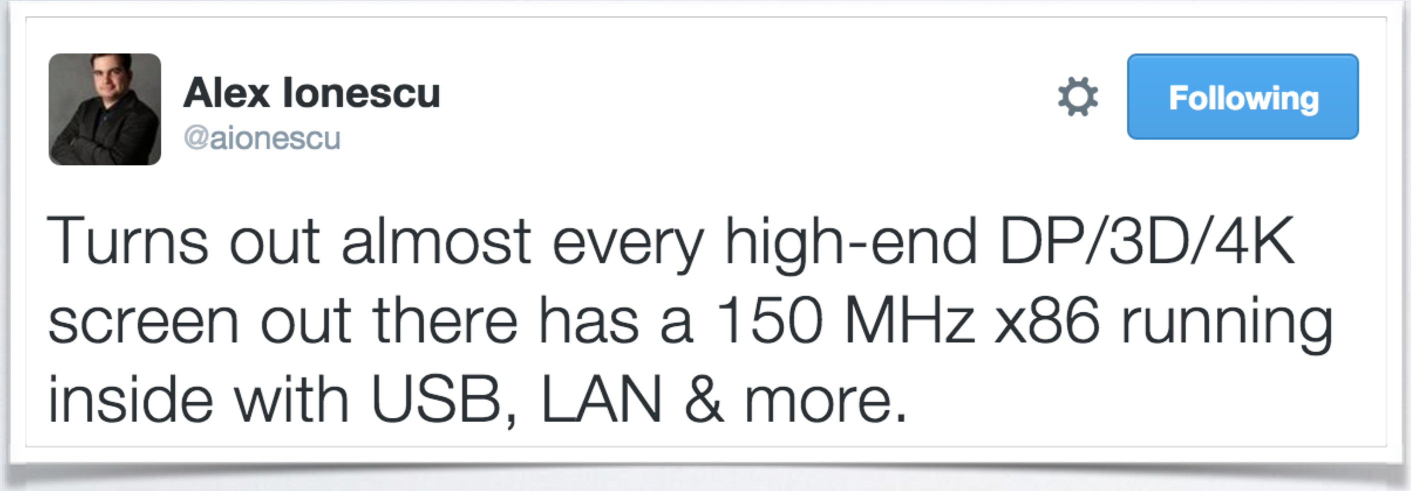
C	95%
16 Other	5%

Lines of Code

https://www.openhub.net/p/linux

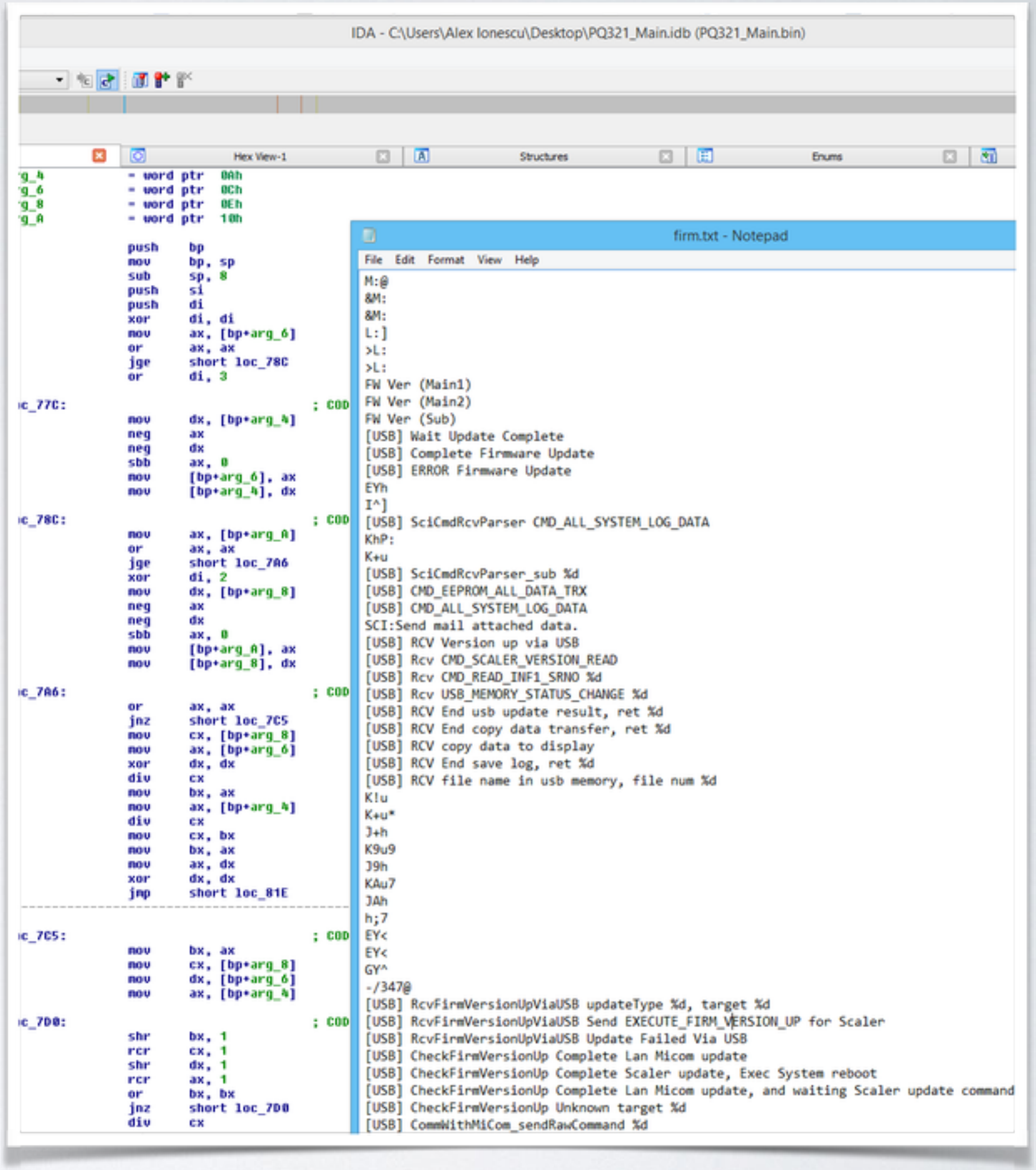
HITACHI

1GB
micro SD



Alex Ionescu
@aionescu

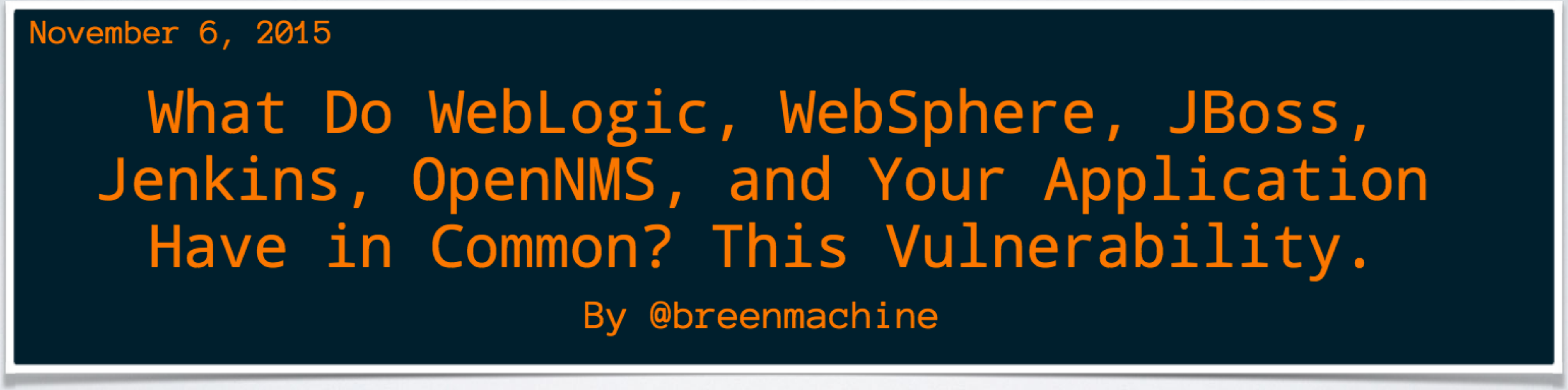
Turns out almost every high-end DP/3D/4K screen out there has a 150 MHz x86 running inside with USB, LAN & more.


IDA - C:\Users\Alex Ionescu\Desktop\PQ321_Main.idb (PQ321_Main.bin)
Hex View-1
Structures
Enums
firm.txt - Notepad
File
Edit
Format
View
Help

```
g_4              = word ptr  0Ah
g_6              = word ptr  0Ch
g_8              = word ptr  0Eh
g_A              = word ptr  10h

                 push    bp
                 mov     bp, sp
                 sub     sp, 8
                 push    si
                 push    di
                 xor     di, di
                 mov     ax, [bp+arg_6]
                 or      ax, ax
                 jge     short loc_78C
                 or      di, 3

c_77C:                                         ; COD
                 mov     dx, [bp+arg_4]
                 neg     ax
                 neg     dx
                 sbb     ax, 0
                 mov     [bp+arg_6], ax
                 mov     [bp+arg_4], dx

c_78C:                                         ; COD
                 mov     ax, [bp+arg_A]
                 or      ax, ax
                 jge     short loc_7A6
                 xor     di, 2
                 mov     dx, [bp+arg_8]
                 neg     ax
                 neg     dx
                 sbb     ax, 0
                 mov     [bp+arg_A], ax
                 mov     [bp+arg_8], dx

c_7A6:                                         ; COD
                 or      ax, ax
                 jnz     short loc_7C5
                 mov     cx, [bp+arg_8]
                 mov     ax, [bp+arg_6]
                 xor     dx, dx
                 div     cx
                 mov     bx, ax
                 mov     ax, [bp+arg_4]
                 div     cx
                 mov     cx, bx
                 mov     bx, ax
                 mov     ax, dx
                 xor     dx, dx
                 jmp     short loc_81E
-----------------------------------------------

c_7C5:                                         ; COD
                 mov     bx, ax
                 mov     cx, [bp+arg_8]
                 mov     dx, [bp+arg_6]
                 mov     ax, [bp+arg_4]

c_7D0:                                         ; COD
                 shr     bx, 1
                 rcr     cx, 1
                 shr     dx, 1
                 rcr     ax, 1
                 or      bx, bx
                 jnz     short loc_7D0
                 div     cx
```

```
M:@
&M:
&M:
L:]
>L:
>L:
FW Ver (Main1)
FW Ver (Main2)
FW Ver (Sub)
[USB] Wait Update Complete
[USB] Complete Firmware Update
[USB] ERROR Firmware Update
EYh
I^]
[USB] SciCmdRcvParser CMD_ALL_SYSTEM_LOG_DATA
KhP:
K+u
[USB] SciCmdRcvParser_sub %d
[USB] CMD_EEPROM_ALL_DATA_TRX
[USB] CMD_ALL_SYSTEM_LOG_DATA
SCI:Send mail attached data.
[USB] RCV Version up via USB
[USB] Rcv CMD_SCALER_VERSION_READ
[USB] Rcv CMD_READ_INF1_SRNO %d
[USB] Rcv USB_MEMORY_STATUS_CHANGE %d
[USB] RCV End usb update result, ret %d
[USB] RCV End copy data transfer, ret %d
[USB] RCV copy data to display
[USB] RCV End save log, ret %d
[USB] RCV file name in usb memory, file num %d
K!u
K+u*
J+h
K9u9
J9h
KAu7
JAh
h;7
EY<
EY<
GY^
-/347@
[USB] RcvFirmVersionUpViaUSB updateType %d, target %d
[USB] RcvFirmVersionUpViaUSB Send EXECUTE_FIRM_VERSION_UP for Scaler
[USB] RcvFirmVersionUpViaUSB Update Failed Via USB
[USB] CheckFirmVersionUp Complete Lan Micom update
[USB] CheckFirmVersionUp Complete Scaler update, Exec System reboot
[USB] CheckFirmVersionUp Complete Lan Micom update, and waiting Scaler update command
[USB] CheckFirmVersionUp Unknown target %d
[USB] CommWithMiCom_sendRawCommand %d
```

https://twitter.com/aionescu/status/615379928305963008



November 6, 2015

What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability.

By @breenmachine

http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/

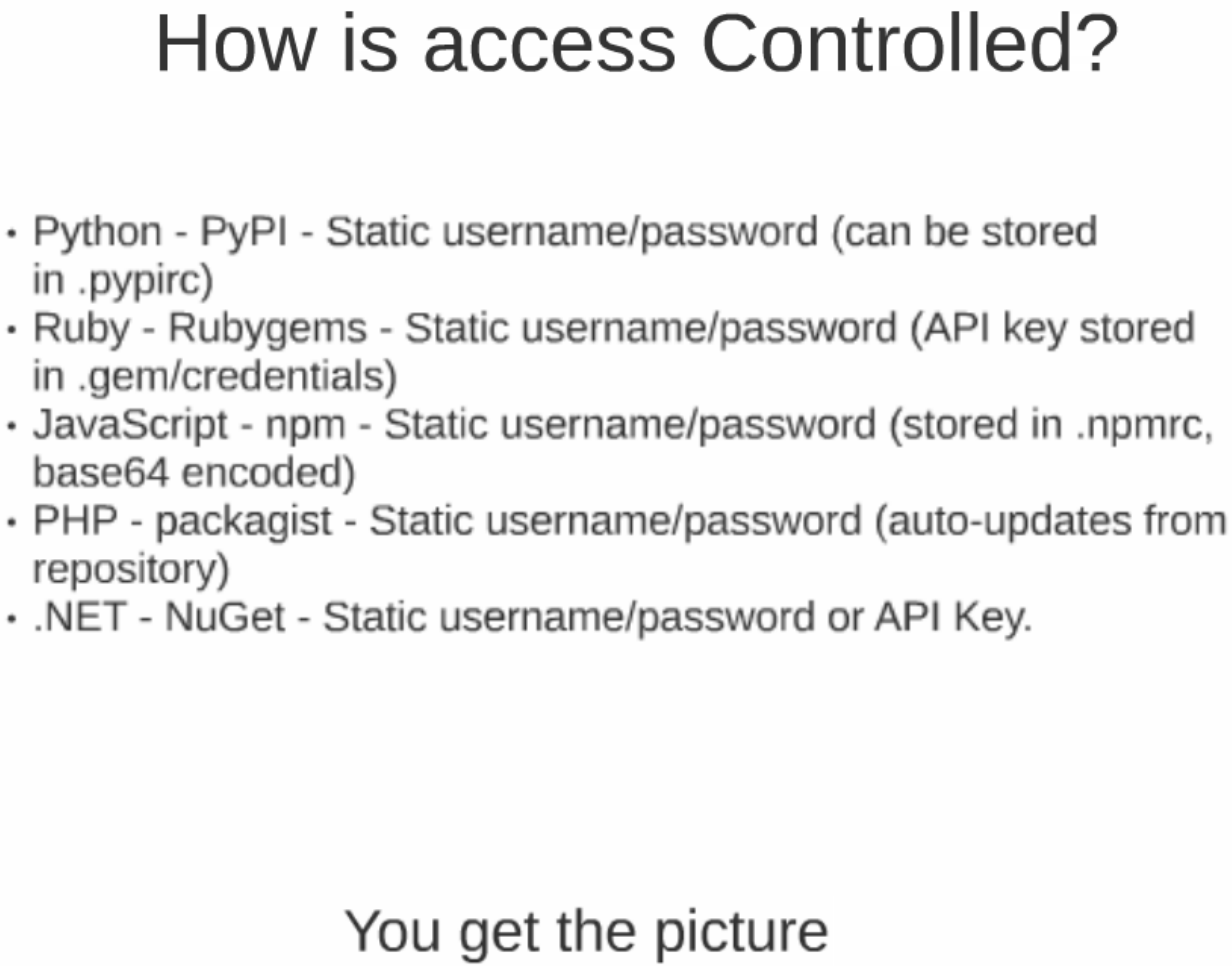
Marshalling Pickles

how deserializing objects can ruin your day

Gabriel Lawrence (@gebl) and Chris Frohoff (@frohoff)

http://www.slideshare.net/frohoff1/appseccali-2015-marshalling-pickles

“‘the Bob Ippolito Problem’’

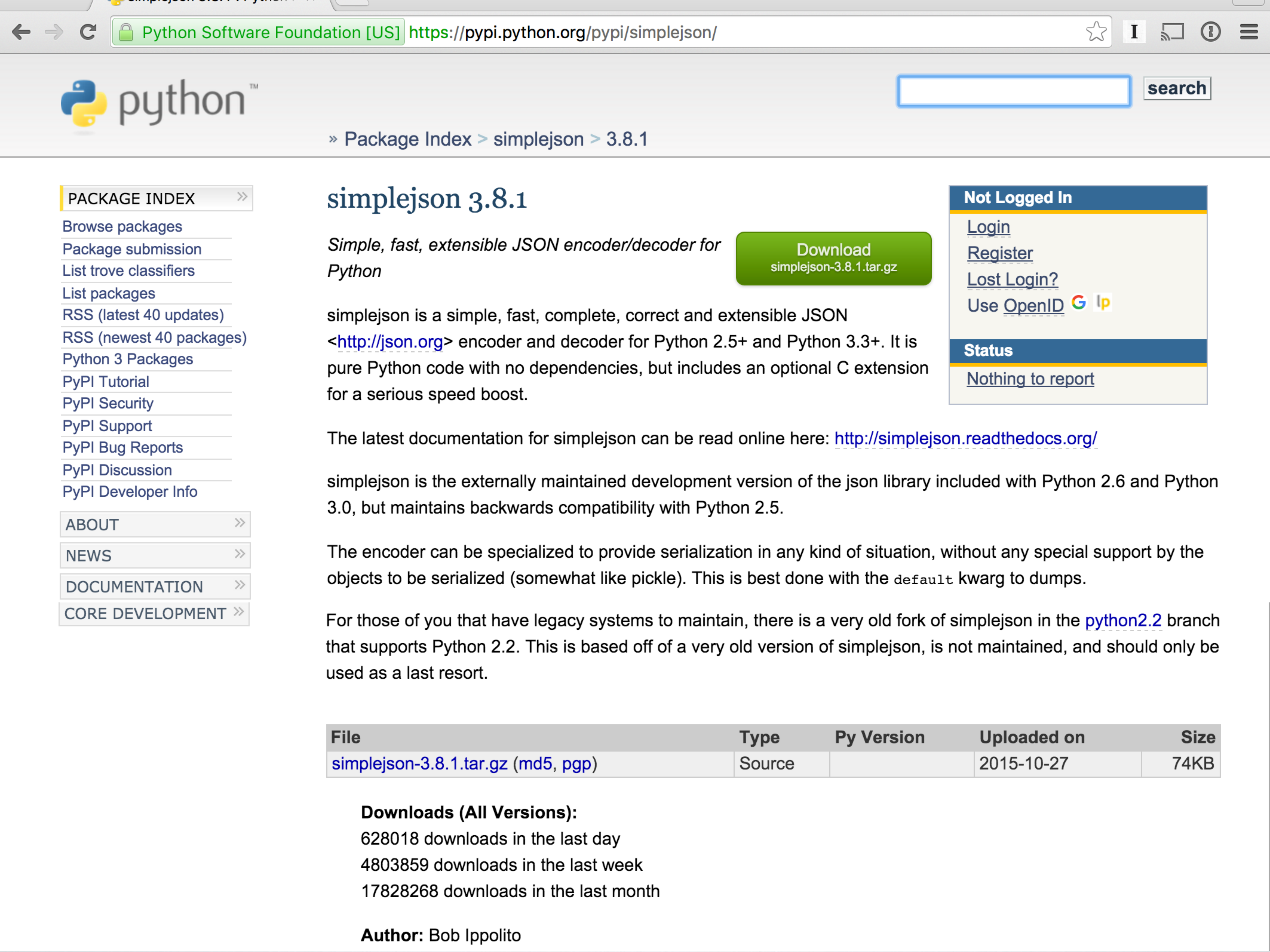


How is access Controlled?

- Python - PyPI - Static username/password (can be stored in .pypirc)
- Ruby - Rubygems - Static username/password (API key stored in .gem/credentials)
- JavaScript - npm - Static username/password (stored in .npmrc, base64 encoded)
- PHP - packagist - Static username/password (auto-updates from repository)
- .NET - NuGet - Static username/password or API Key.

You get the picture

https://prezi.com/vjjq6n2x72ko/security-and-modern-software-deployment-owasp-edition/



simplejson 3.8.1

Simple, fast, extensible JSON encoder/decoder for Python

simplejson is a simple, fast, complete, correct and extensible JSON <http://json.org> encoder and decoder for Python 2.5+ and Python 3.3+. It is pure Python code with no dependencies, but includes an optional C extension for a serious speed boost.

The latest documentation for simplejson can be read online here: http://simplejson.readthedocs.org/

simplejson is the externally maintained development version of the json library included with Python 2.6 and Python 3.0, but maintains backwards compatibility with Python 2.5.

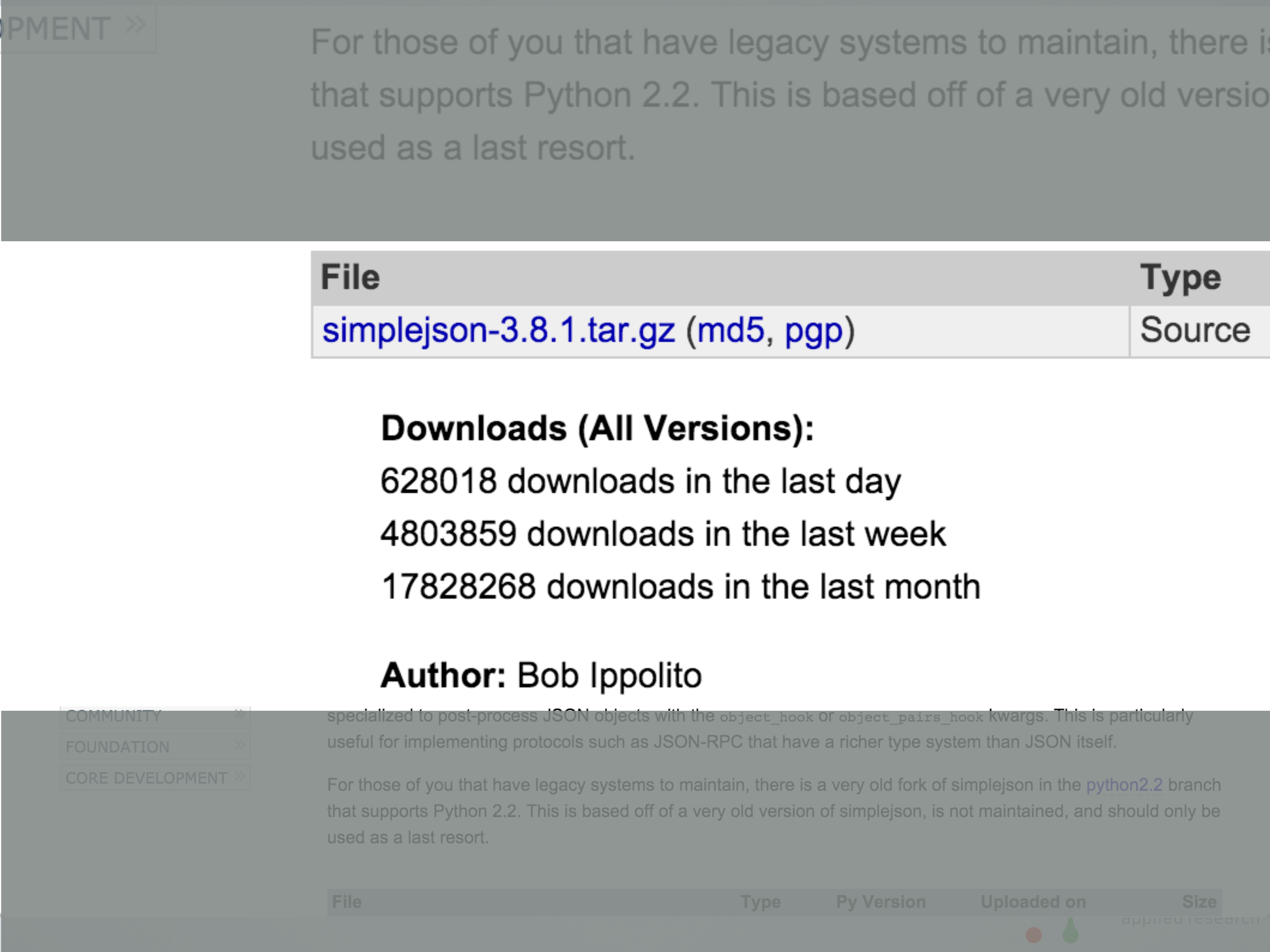
The encoder can be specialized to provide serialization in any kind of situation, without any special support by the objects to be serialized (somewhat like pickle). This is best done with the `default` kwarg to dumps.

For those of you that have legacy systems to maintain, there is a very old fork of simplejson in the python2.2 branch that supports Python 2.2. This is based off of a very old version of simplejson, is not maintained, and should only be used as a last resort.

File	Type	Py Version	Uploaded on	Size
simplejson-3.8.1.tar.gz (md5, pgp)	Source		2015-10-27	74KB

Downloads (All Versions):
628018 downloads in the last day
4803859 downloads in the last week
17828268 downloads in the last month

Author: Bob Ippolito



For those of you that have legacy systems to maintain, there i

that supports Python 2.2. This is based off of a very old versio

used as a last resort.

File	Type
simplejson-3.8.1.tar.gz (md5, pgp)	Source

Downloads (All Versions):

628018 downloads in the last day

4803859 downloads in the last week

17828268 downloads in the last month

Author: Bob Ippolito

specialized to post-process JSON objects with the `object_hook` or `object_pairs_hook` kwargs. This is particularly useful for implementing protocols such as JSON-RPC that have a richer type system than JSON itself.

For those of you that have legacy systems to maintain, there is a very old fork of simplejson in the python2.2 branch that supports Python 2.2. This is based off of a very old version of simplejson, is not maintained, and should only be used as a last resort.

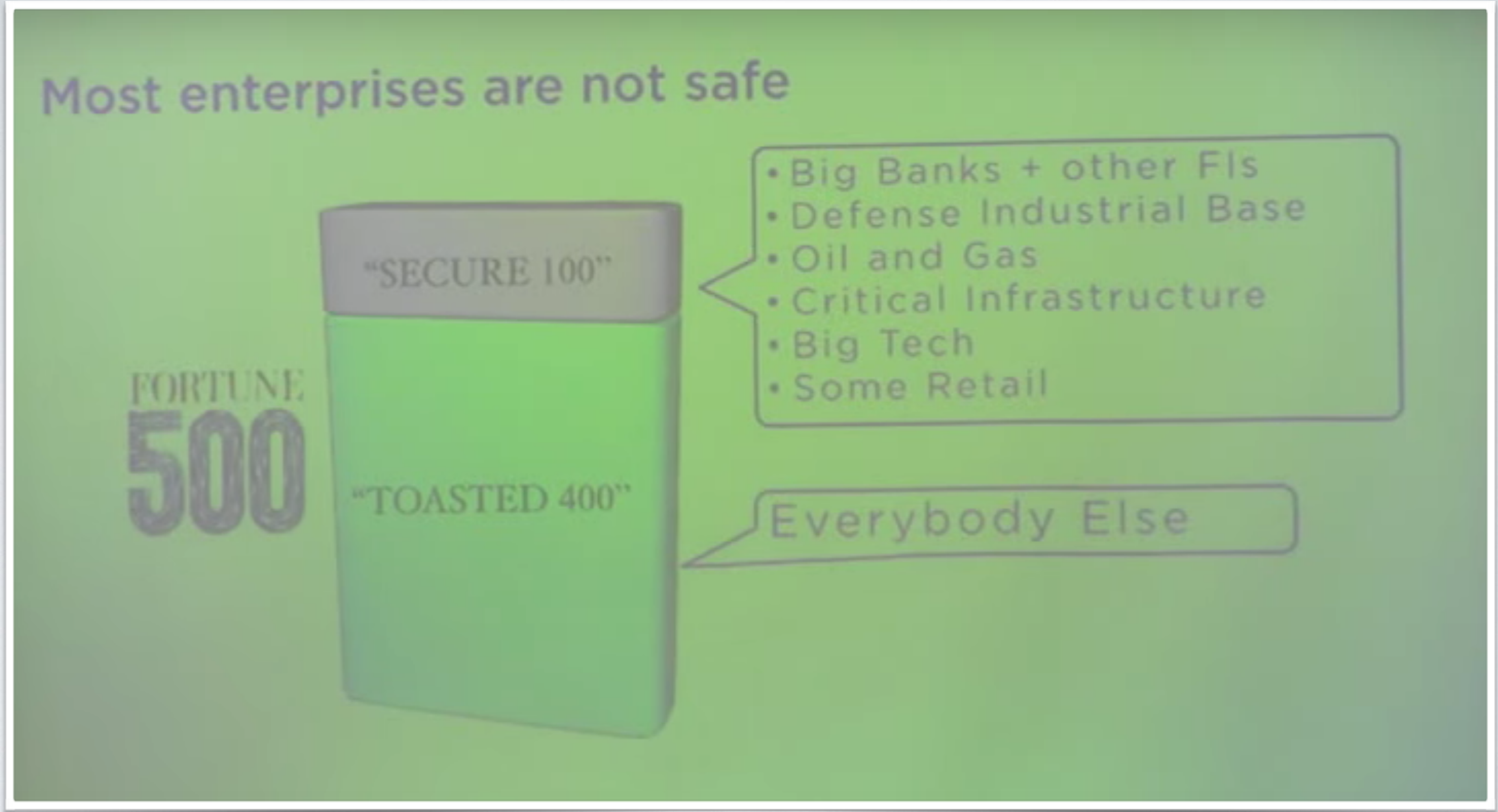
File	Type	Py Version	Uploaded on	Size

“In a composite system there is no critical gate, everything is a gate”

http://recurity-labs.com/content/pub/Lindner_Gaycken-Back-to-Basics.pdf

thinkst
applied research

We are in bad shape;
It’s going to get much worse..
and..



Most enterprises are not safe

FORTUNE 500

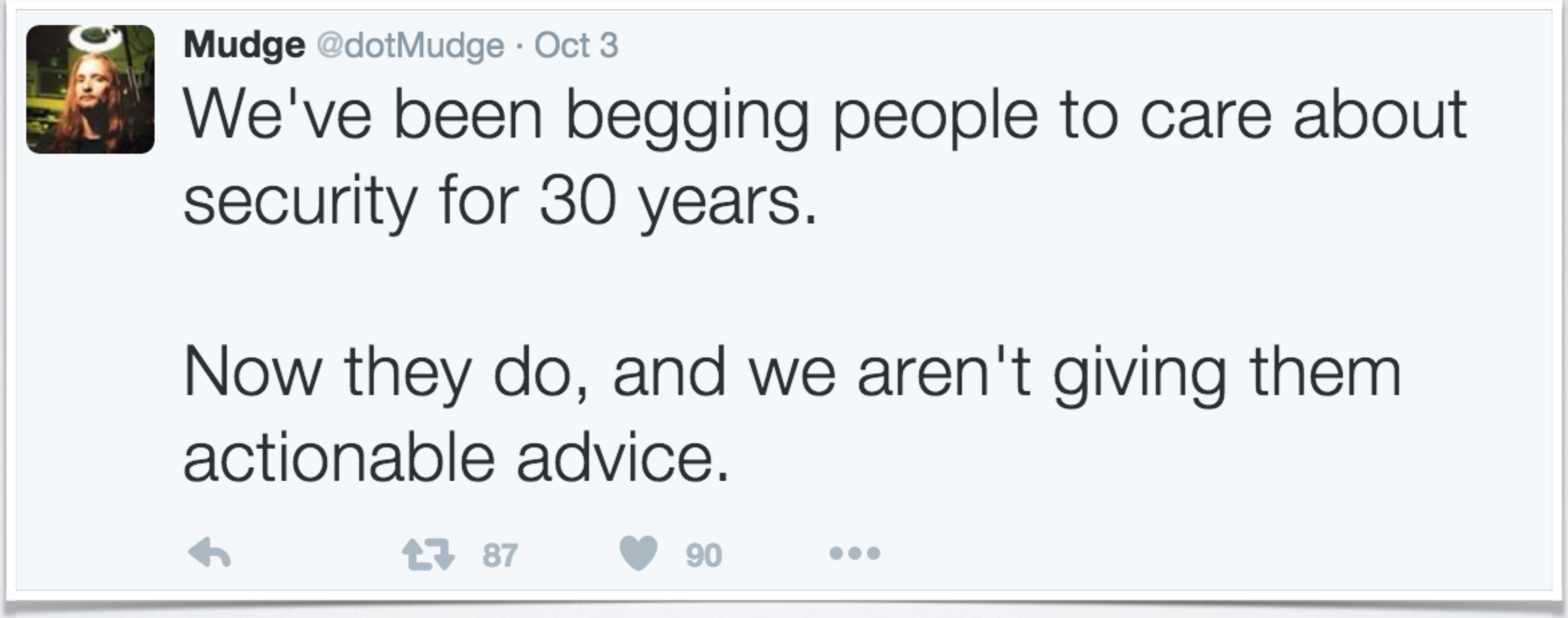
"SECURE 100"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

"TOASTED 400"

Everybody Else

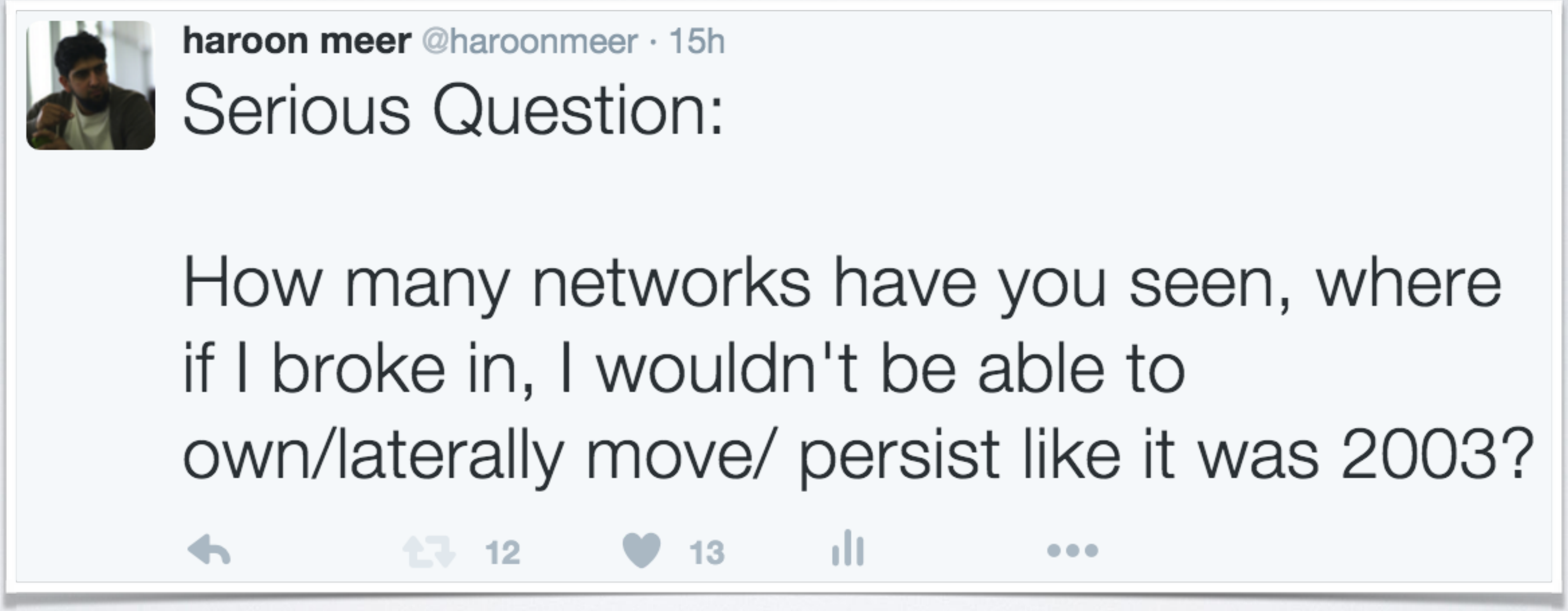
https://www.youtube.com/watch?v=-1kZMn1RueI



Mudge @dotMudge · Oct 3

We've been begging people to care about security for 30 years.

Now they do, and we aren't giving them actionable advice.



haroon meer @haroonmeer · 15h

Serious Question:

How many networks have you seen, where if I broke in, I wouldn't be able to own/laterally move/ persist like it was 2003?

thinkst
applied research

What have we been doing for the past 15 years?

We wanted to make a difference?

“At least we are doing something!”

(thats better than nothing, right?)

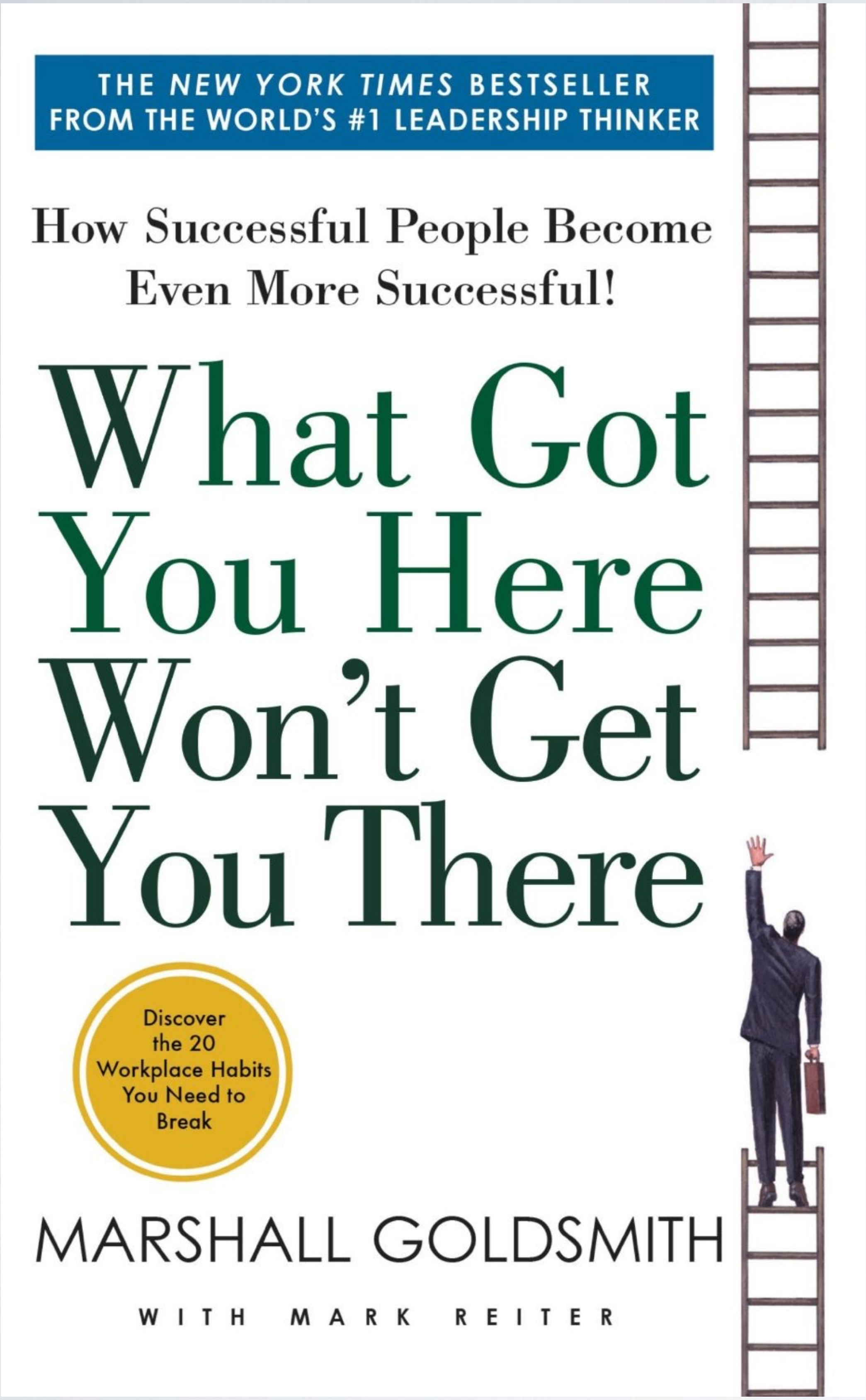
"'Wrong! Peddling hard in the wrong direction doesn't help just because you want it to"

http://blog.thinkst.com/2013/01/your-companies-security-posture-is.html

thinkst
applied research

“If you want something new, you have to stop doing something old.”

- Peter Drucker



THE *NEW YORK TIMES* BESTSELLER
FROM THE WORLD'S #1 LEADERSHIP THINKER

How Successful People Become
Even More Successful!

What Got
You Here
Won't Get
You There

Discover
the 20
Workplace Habits
You Need to
Break

MARSHALL GOLDSMITH

WITH MARK REITER

"We spend a lot of time helping Leaders learn what to do. We don't spend enough time helping them learn what to stop.”

The 20 Habits that hold us Back

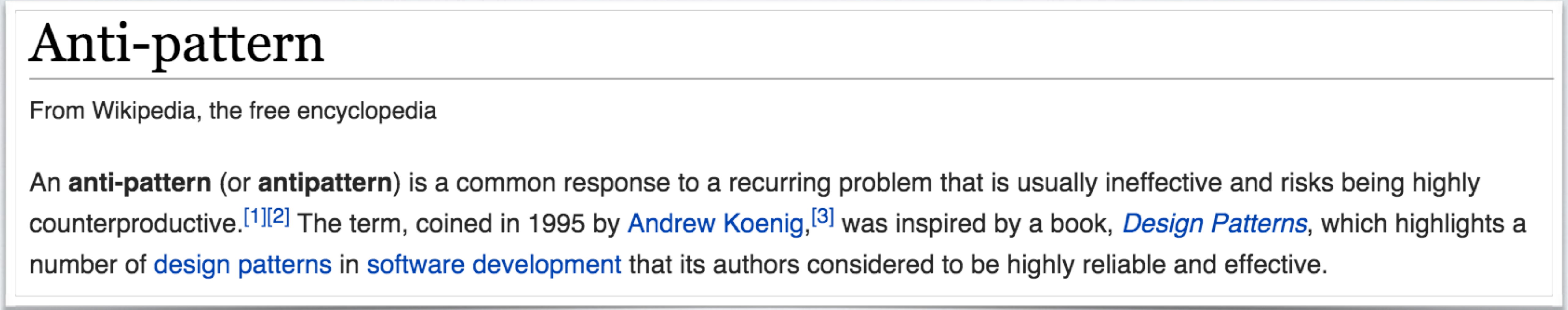
1) …
2) …
3) Passing Judgement
4) Making Destructive Comments
5) Starting with “No”, “But”, “However”
6) Telling the world how smart we are
7) Speaking when angry
8) Negativity, or “let me explain why that wont work”
9) …
10) …

The 20 Habits that hold us Back

10) …
11) Claiming credit we don't deserve
12) Making excuses
13) Clinging to the past
14) …
15) …
16) Not Listening
17) …
18) …
19) Passing the buck
20) …

thinkst
applied research

Security Anti-Patterns



Anti-pattern

From Wikipedia, the free encyclopedia

An **anti-pattern** (or **antipattern**) is a common response to a recurring problem that is usually ineffective and risks being highly counterproductive.[1][2] The term, coined in 1995 by Andrew Koenig,[3] was inspired by a book, *Design Patterns*, which highlights a number of design patterns in software development that its authors considered to be highly reliable and effective.

Taken some wrong turns;

□ Developed some bad habits;

□ Missing some opportunities.

Penetration Testing

WRONG WAY

https://www.youtube.com/watch?v=GvX52HPAfBk

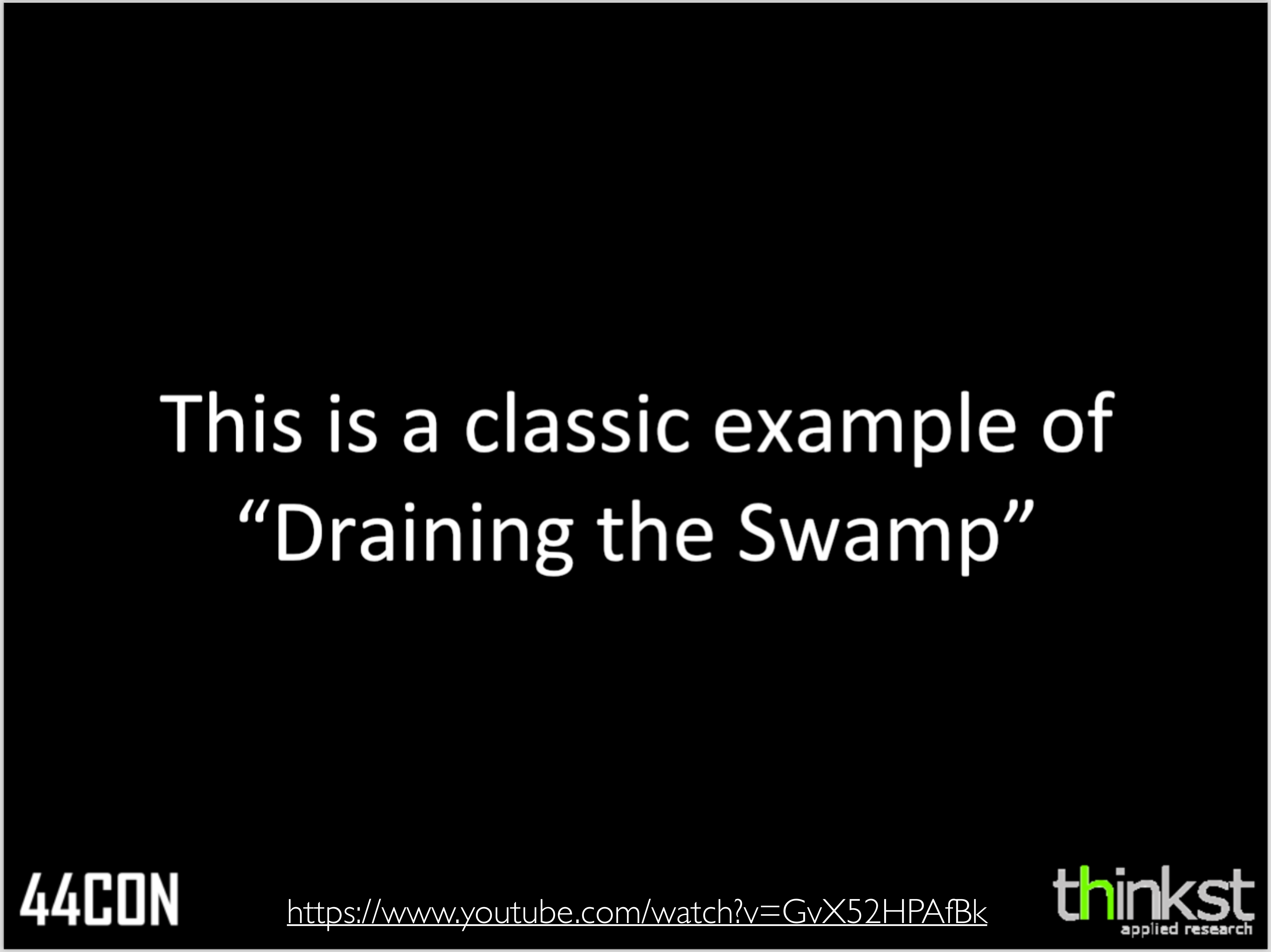
thinkst
applied research

Web browsers are a constant target for attack..

When last have you used one on a pen-test?

These days we just simulate other pen-testers..

https://www.youtube.com/watch?v=GvX52HPAfBk



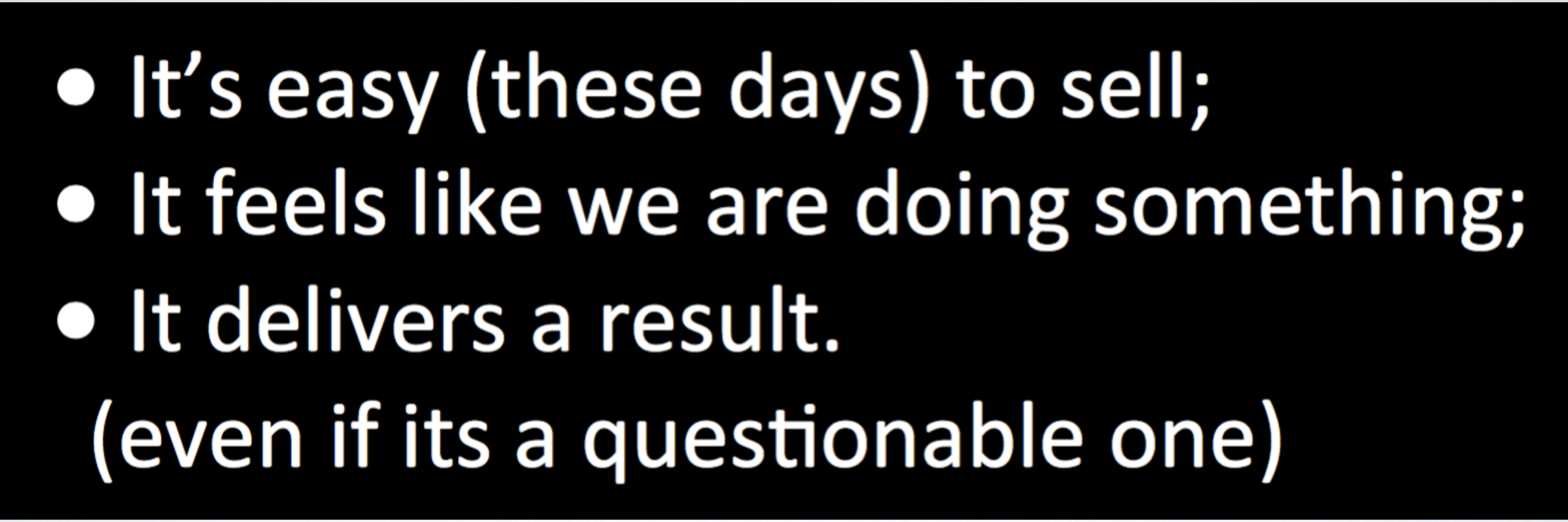
This is a classic example of
“Draining the Swamp”

https://www.youtube.com/watch?v=GvX52HPAfBk

WRONG WAY

https://www.youtube.com/watch?v=GvX52HPAfBk

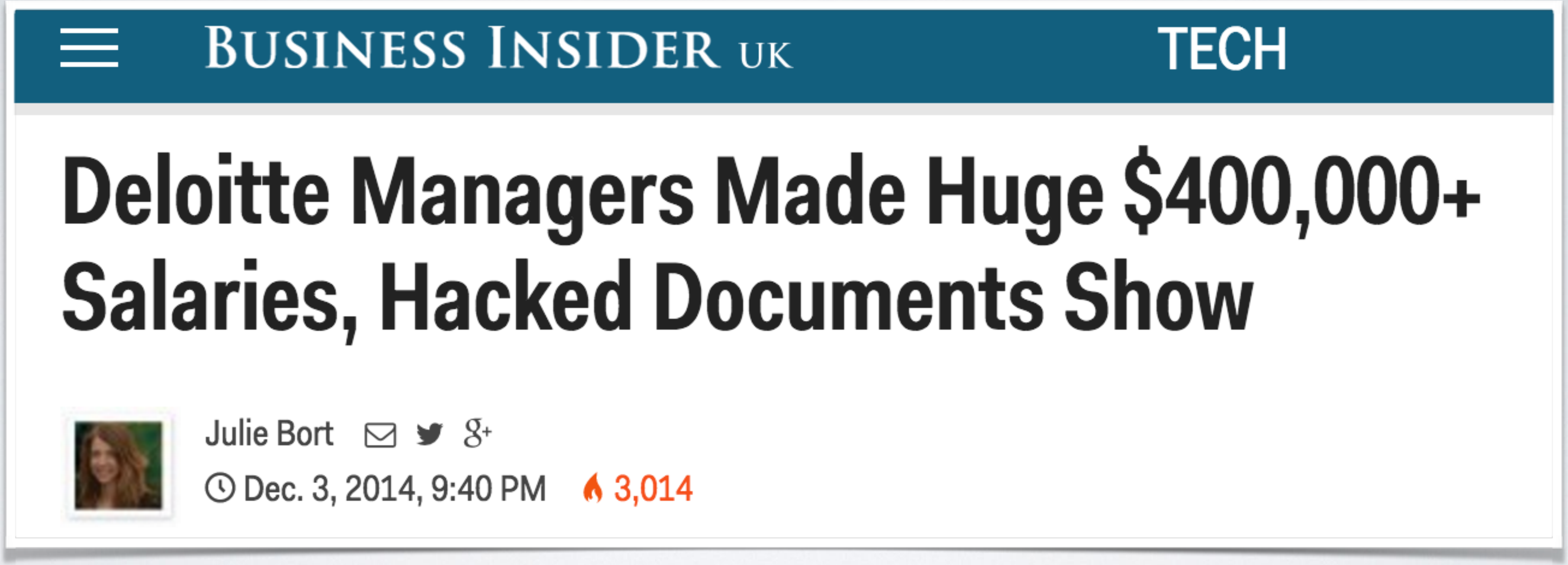
Possible to be perfectly pleased,
perfectly pwned,
and still be perfectly pwnable!



- It’s easy (these days) to sell;
- It feels like we are doing something;
- It delivers a result.

(even if its a questionable one)

how do we define risk in an org?



BUSINESS INSIDER UK

TECH

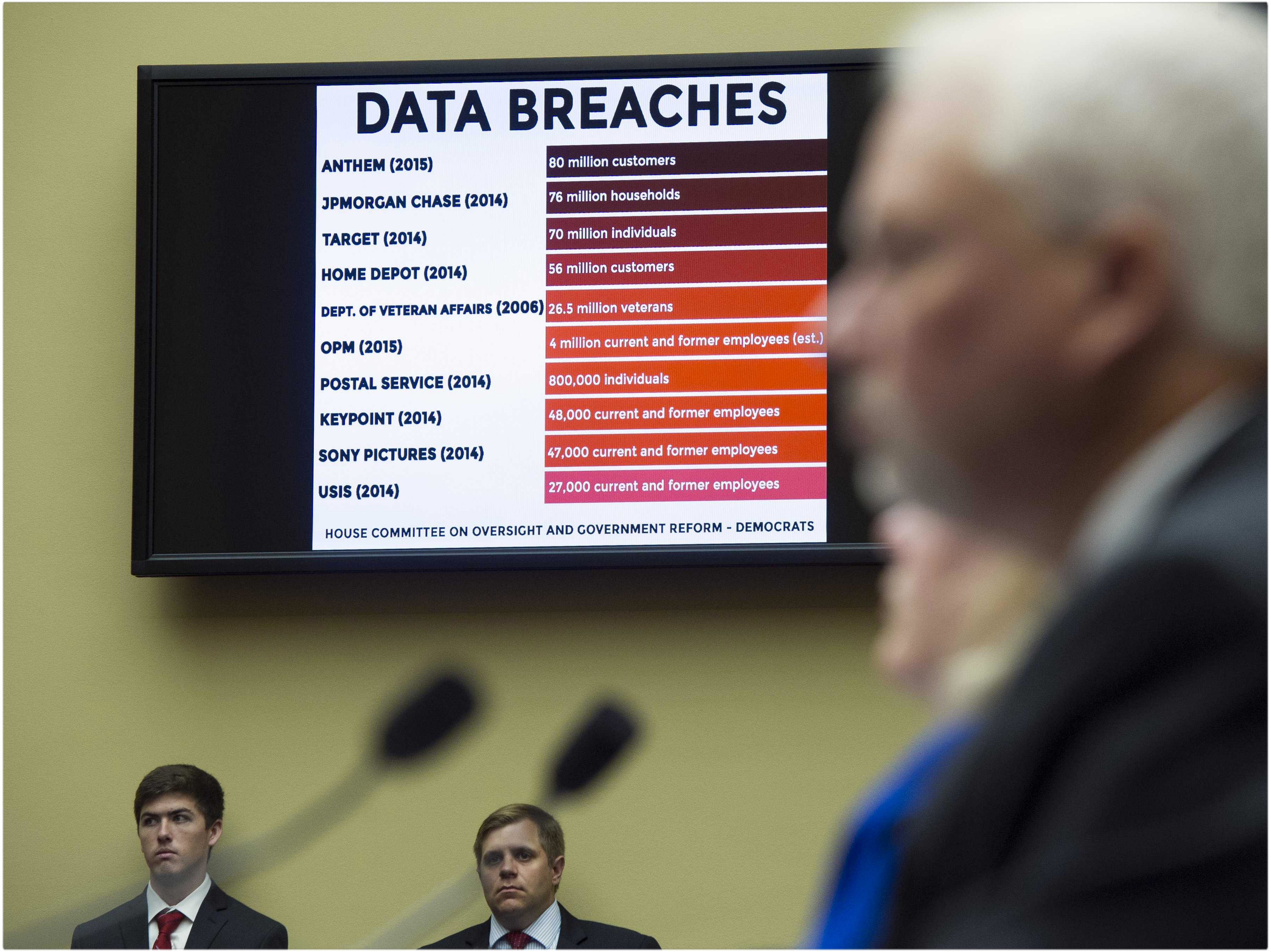
Deloitte Managers Made Huge $400,000+ Salaries, Hacked Documents Show

Julie Bort

Dec. 3, 2014, 9:40 PM 3,014

http://uk.businessinsider.com/sony-hack-reveals-huge-deloitte-salaries-2014-12?r=US&IR=T

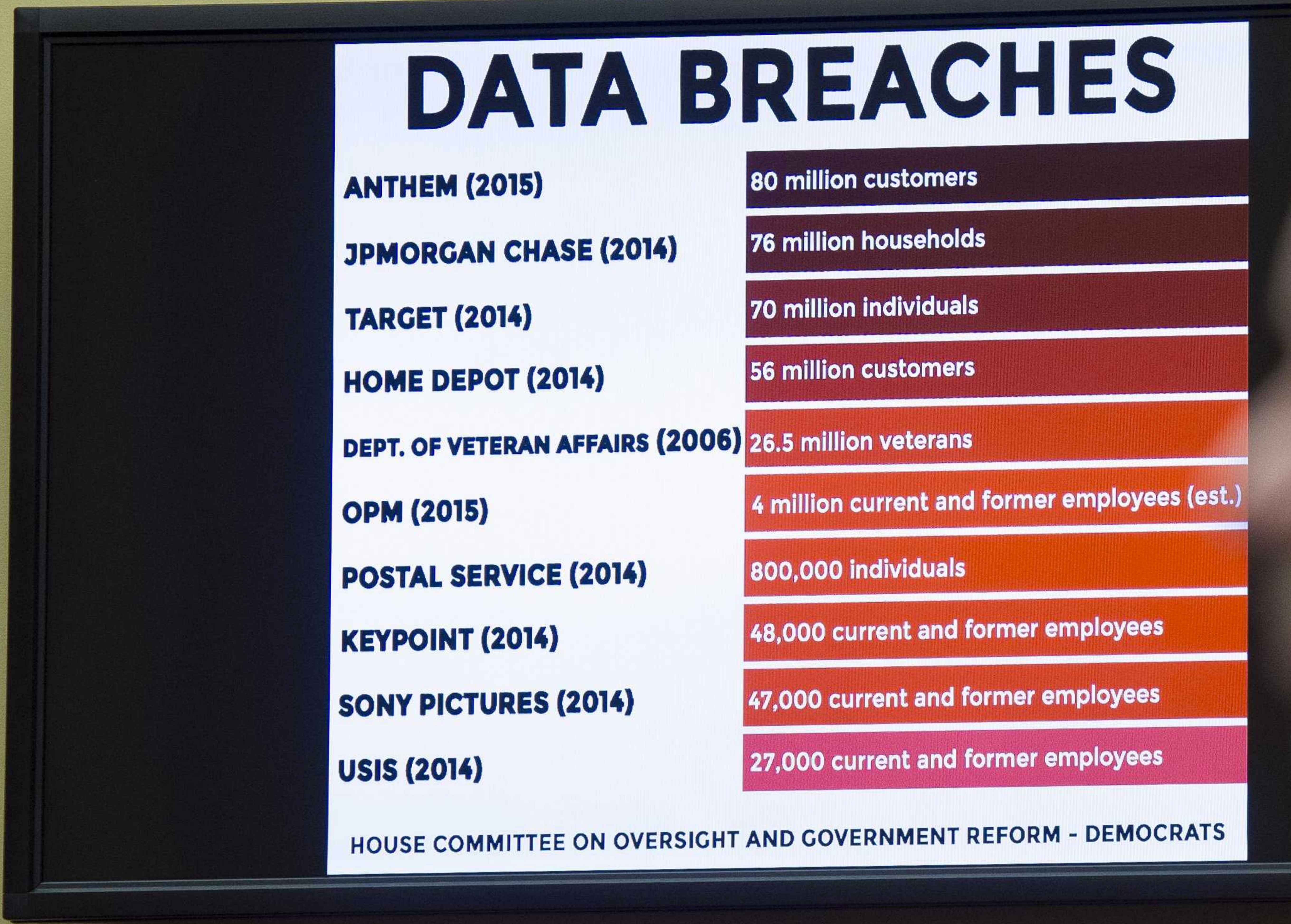
how do we define risk in an org?



DATA BREACHES

ANTHEM (2015)	80 million customers
JPMORGAN CHASE (2014)	76 million households
TARGET (2014)	70 million individuals
HOME DEPOT (2014)	56 million customers
DEPT. OF VETERAN AFFAIRS (2006)	26.5 million veterans
OPM (2015)	4 million current and former employees (est.)
POSTAL SERVICE (2014)	800,000 individuals
KEYPOINT (2014)	48,000 current and former employees
SONY PICTURES (2014)	47,000 current and former employees
USIS (2014)	27,000 current and former employees

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM - DEMOCRATS



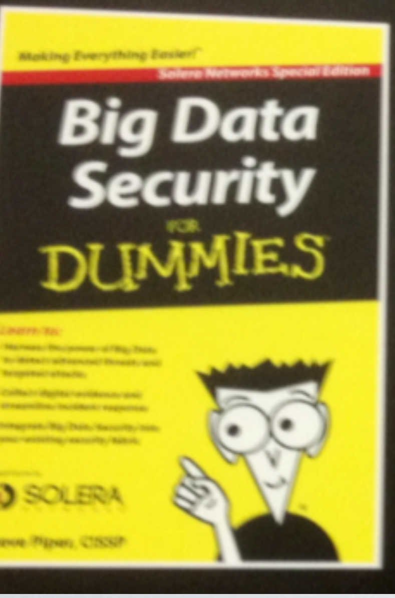
DATA BREACHES

ANTHEM (2015)	80 million customers
JPMORGAN CHASE (2014)	76 million households
TARGET (2014)	70 million individuals
HOME DEPOT (2014)	56 million customers
DEPT. OF VETERAN AFFAIRS (2006)	26.5 million veterans
OPM (2015)	4 million current and former employees (est.)
POSTAL SERVICE (2014)	800,000 individuals
KEYPOINT (2014)	48,000 current and former employees
SONY PICTURES (2014)	47,000 current and former employees
USIS (2014)	27,000 current and former employees

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM - DEMOCRATS

RSA®
CONFERENCE
2013
FEBRUARY 25 – MARCH 1
SAN FRANCISCO

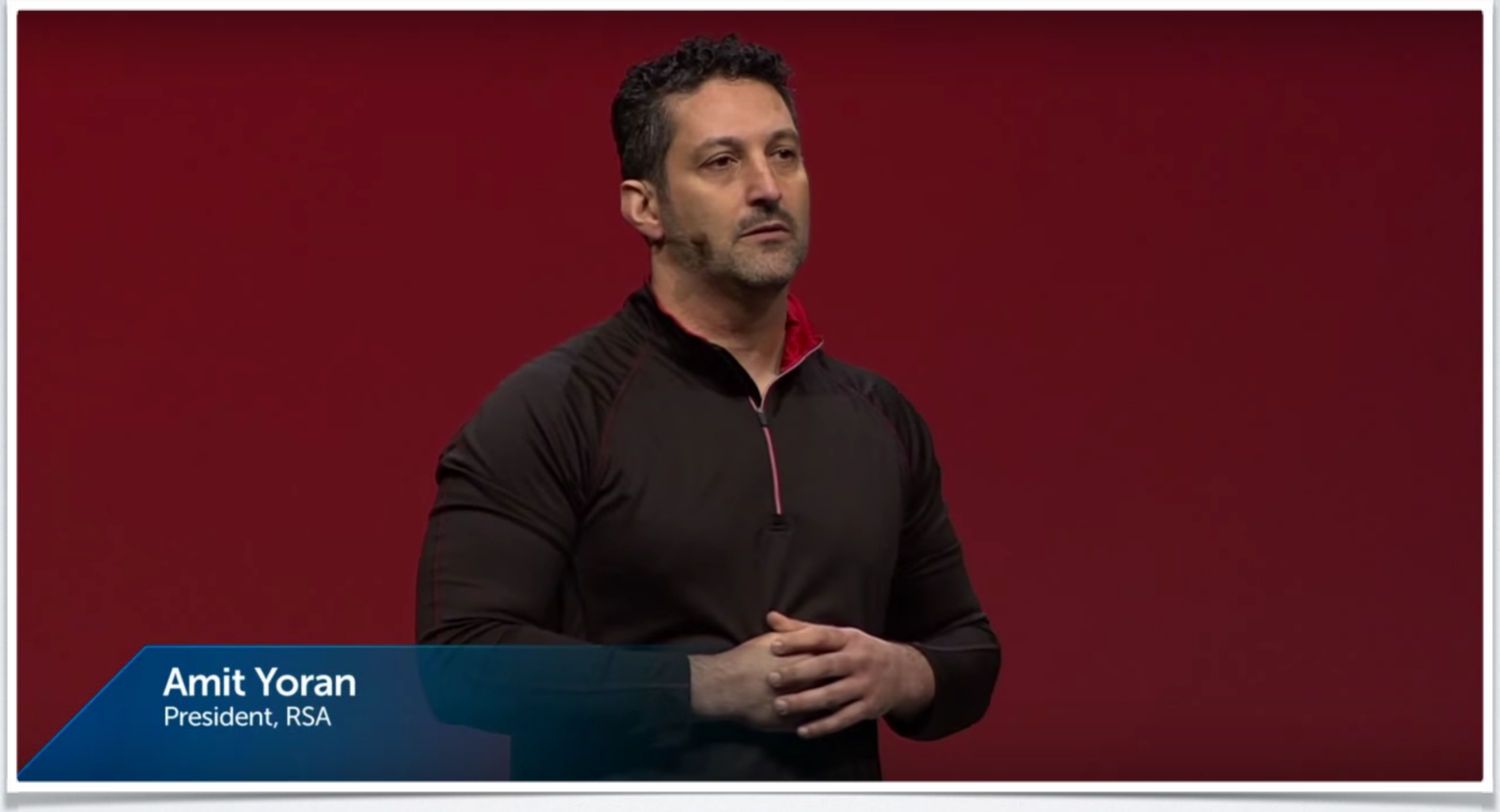
TAKE THE BIG DATA SECURITY CHALLENGE



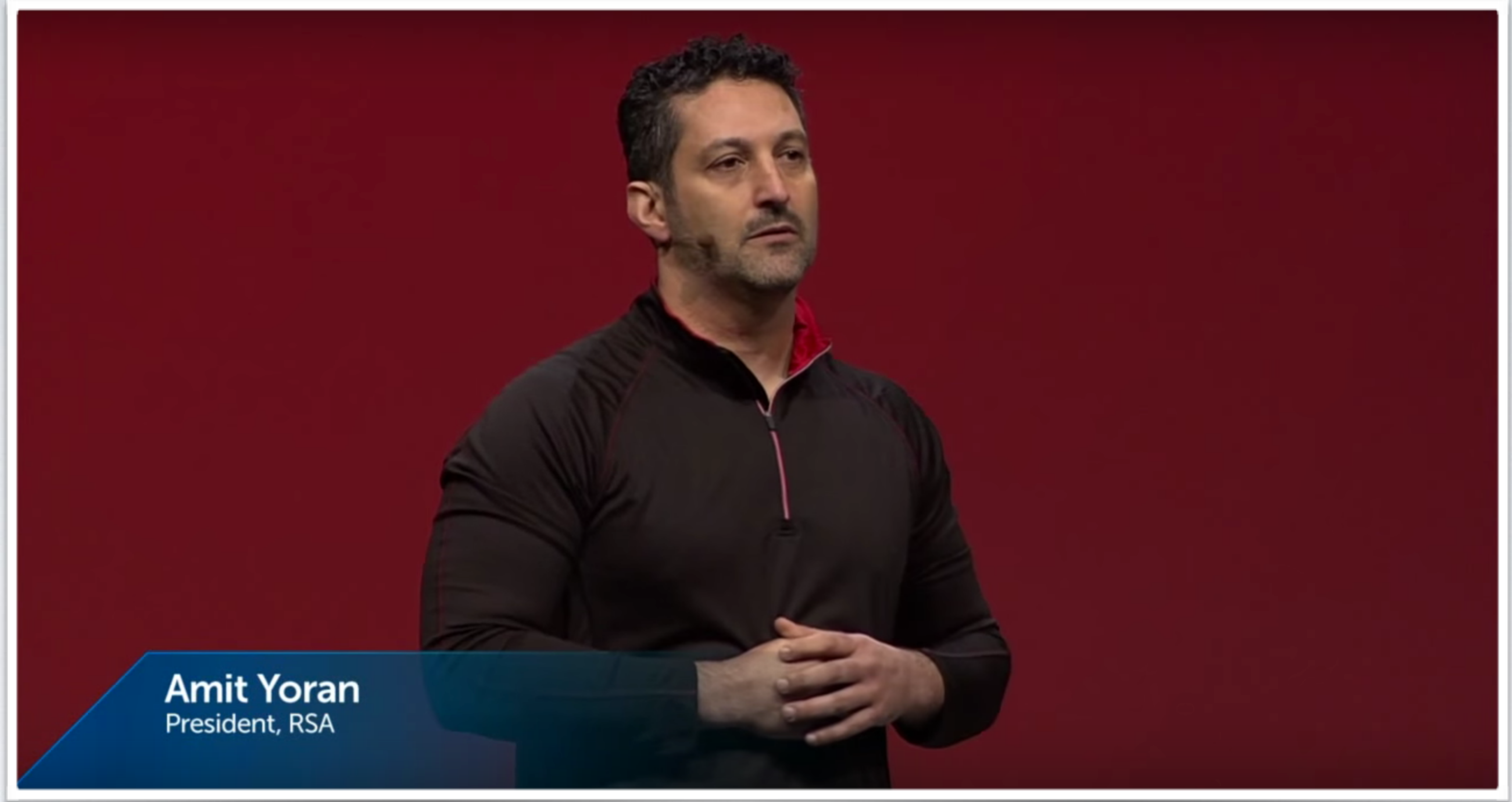
Brought to you by Solera Networks!

Threat Intelligence
&
Information Sharing

https://www.youtube.com/watch?v=op-2Aj6Wizo



“Consider STUXNET, EquationGroup, These intrusion sets and countless others from sophisticated adversaries.. One of their defining characteristics is the fact that they are stealthy, they evade detection. Until written about, they are virtually undetectable, because they bypass traditional defences.”



“We need pervasive and true visibility into our enterprise environments. These aren't nice to haves.. They are foundational, core requirements for any modern security program”

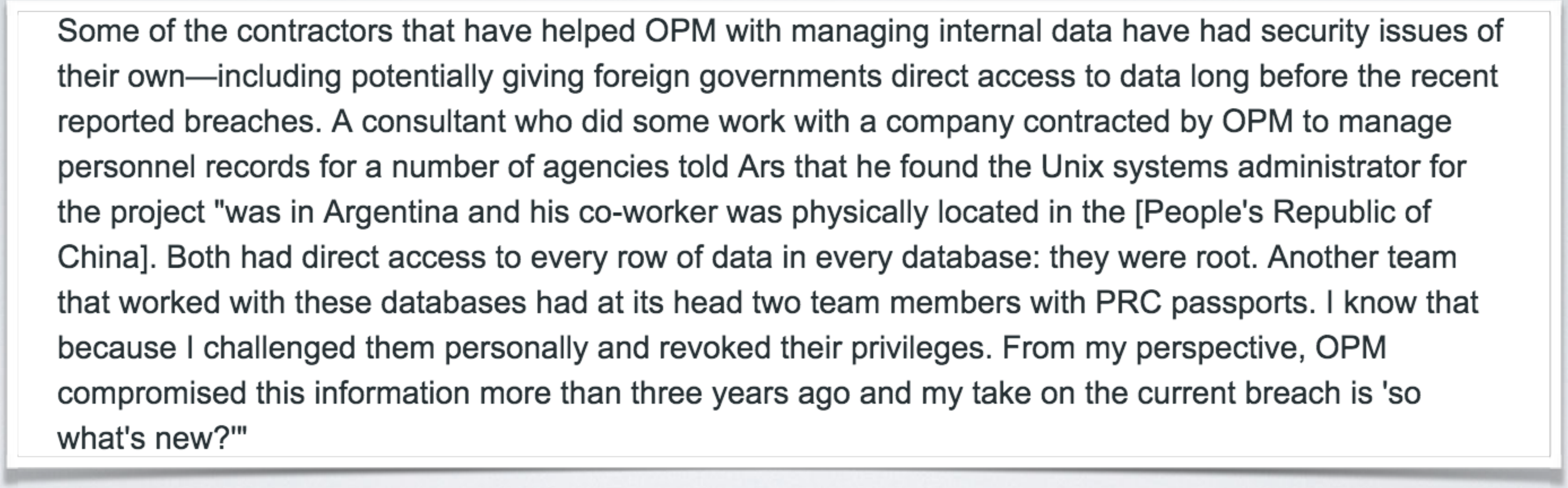
“If you don't have that level of security, you are only pretending to do security”

“‘threat intelligence.. another core requirement’’
‘‘so analysts can mostly quickly respond and identify those threats that matter most to the organisation"

Perfectly Typical

WRONG WAY

UNITED STATES
OFFICE OF
SONN
MANA
MANAGEMENT
TARGET
SONY



Some of the contractors that have helped OPM with managing internal data have had security issues of their own—including potentially giving foreign governments direct access to data long before the recent reported breaches. A consultant who did some work with a company contracted by OPM to manage personnel records for a number of agencies told Ars that he found the Unix systems administrator for the project "was in Argentina and his co-worker was physically located in the [People's Republic of China]. Both had direct access to every row of data in every database: they were root. Another team that worked with these databases had at its head two team members with PRC passports. I know that because I challenged them personally and revoked their privileges. From my perspective, OPM compromised this information more than three years ago and my take on the current breach is 'so what's new?'"

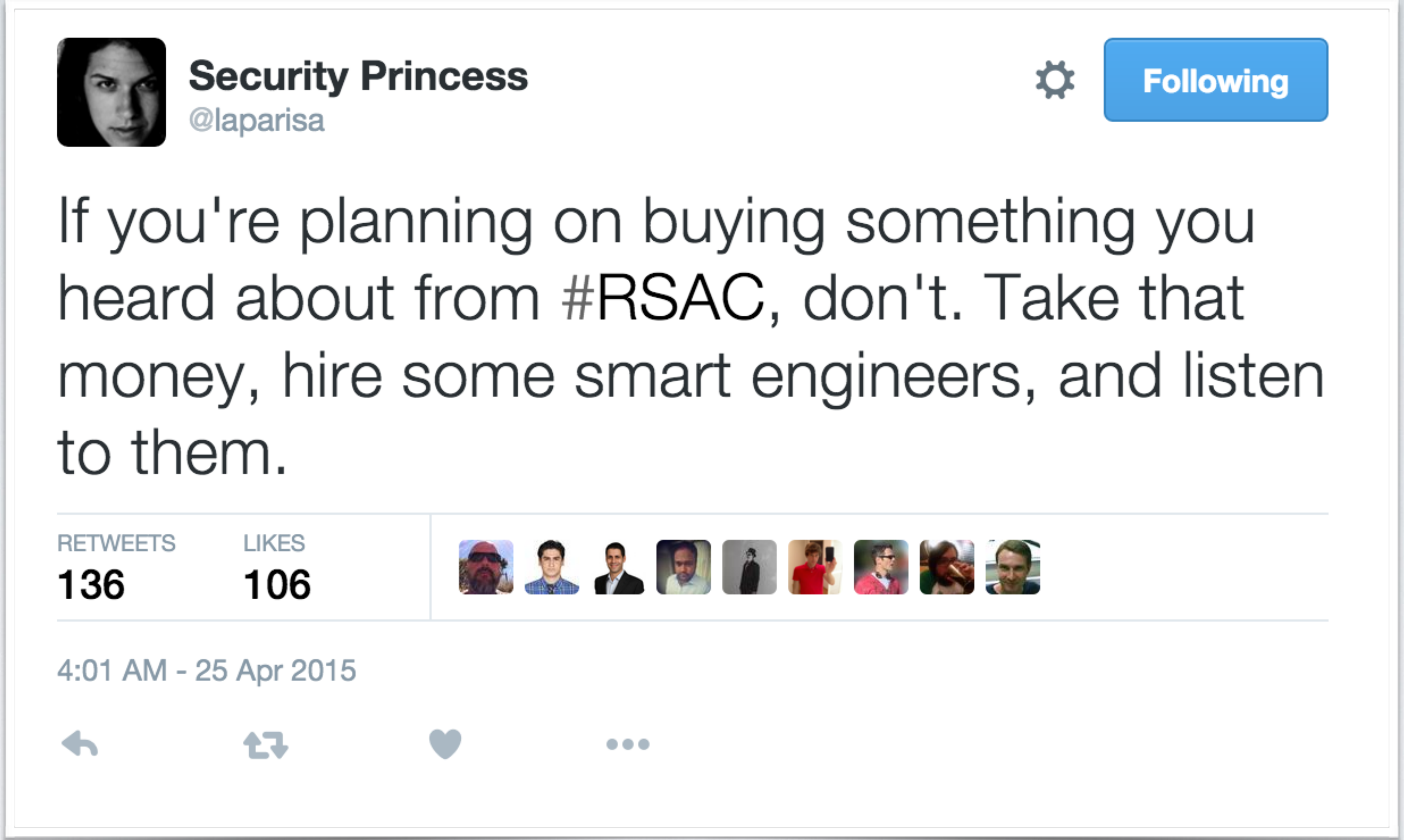
the Unix systems administrator for the project "was in Argentina and his co-worker was physically located in the [People's Republic of China]. Both had direct access to every row of data in every database: they were root"

http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/

But what's wrong with learning about malicious activity on other networks in near real time?

Before near-real-time learning..
how about 6-year old learning?

thinkst
applied research



Security Princess
@laparisa

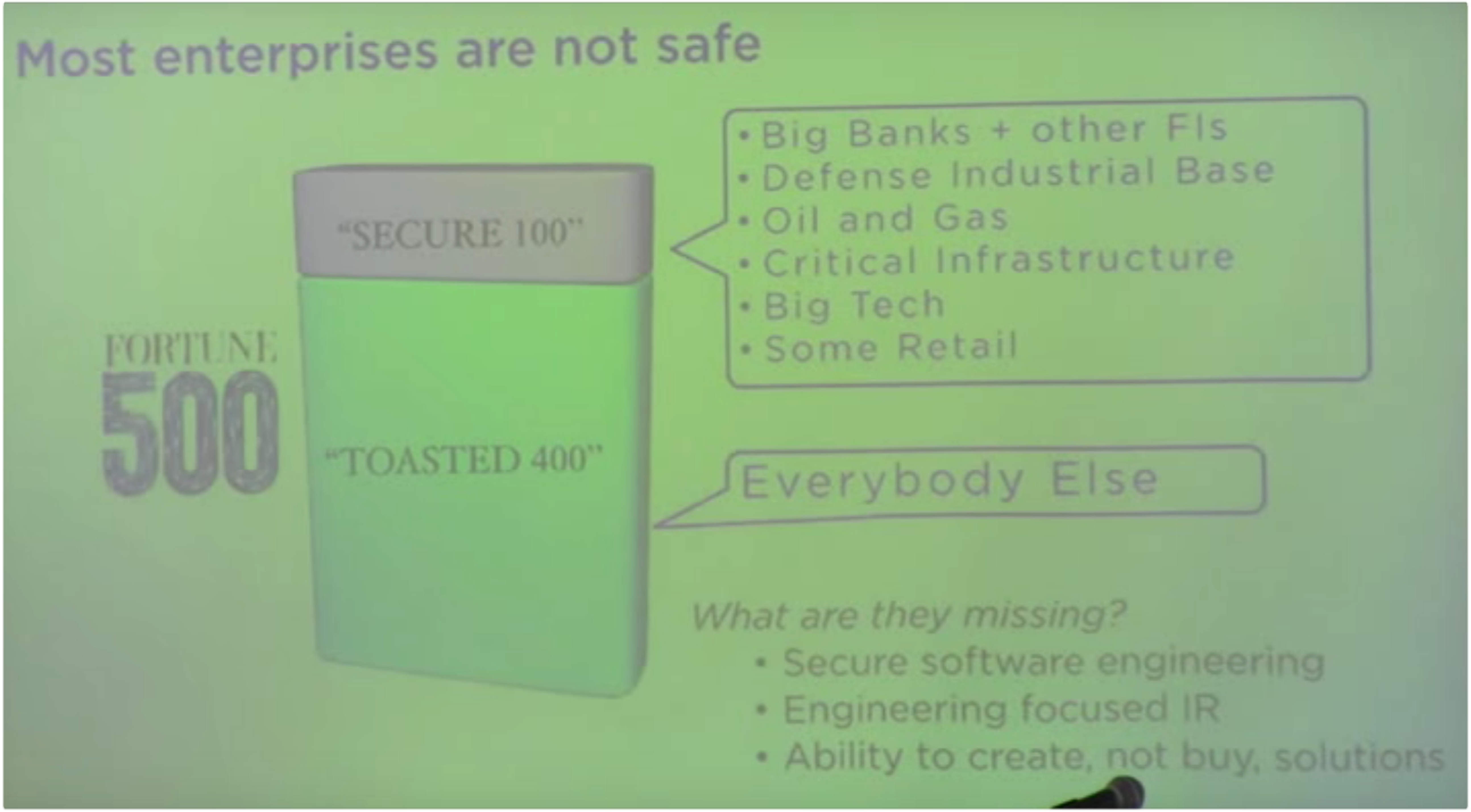
If you're planning on buying something you heard about from #RSAC, don't. Take that money, hire some smart engineers, and listen to them.

RETWEETS 136
LIKES 106

4:01 AM - 25 Apr 2015

WRONG WAY

https://twitter.com/laparisa/status/591784079969755136



Most enterprises are not safe

FORTUNE 500

"SECURE 100"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

"TOASTED 400"

Everybody Else

What are they missing?

- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

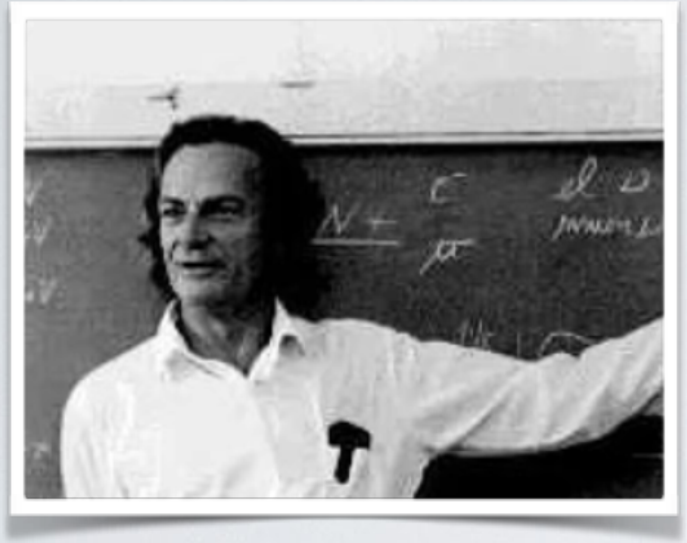
https://www.youtube.com/watch?v=-1kZMn1RueI

“Cant we just use consultants?”

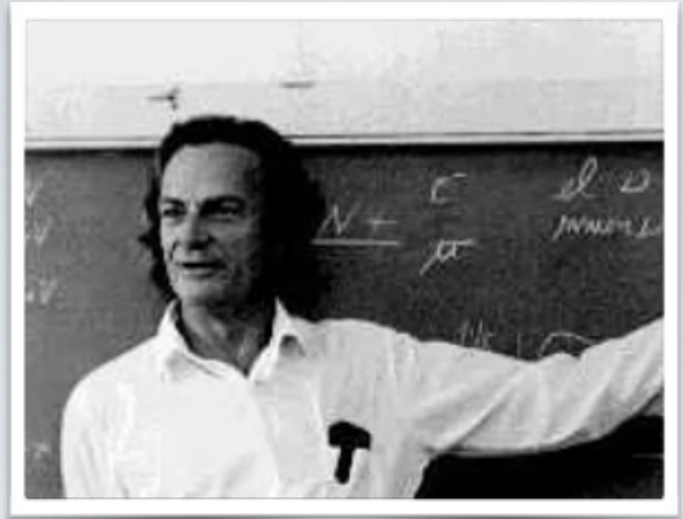
You can’t outsource your thinking!

"Understand your prize jewels"

WRONG WAY



Cargo Cult Science



Cargo Cult Security

Taken some wrong turns;

Developed some bad habits;

Missing some opportunities.

““it’s not perfect, throw it out!””

thinkst
applied research

https://www.youtube.com/watch?v=kBHAUs1jDJk

Enhanced
Mitigation
Experience
Toolkit

Bring back the Honeypots

{marco|haroon|azhar}@thinkst.com

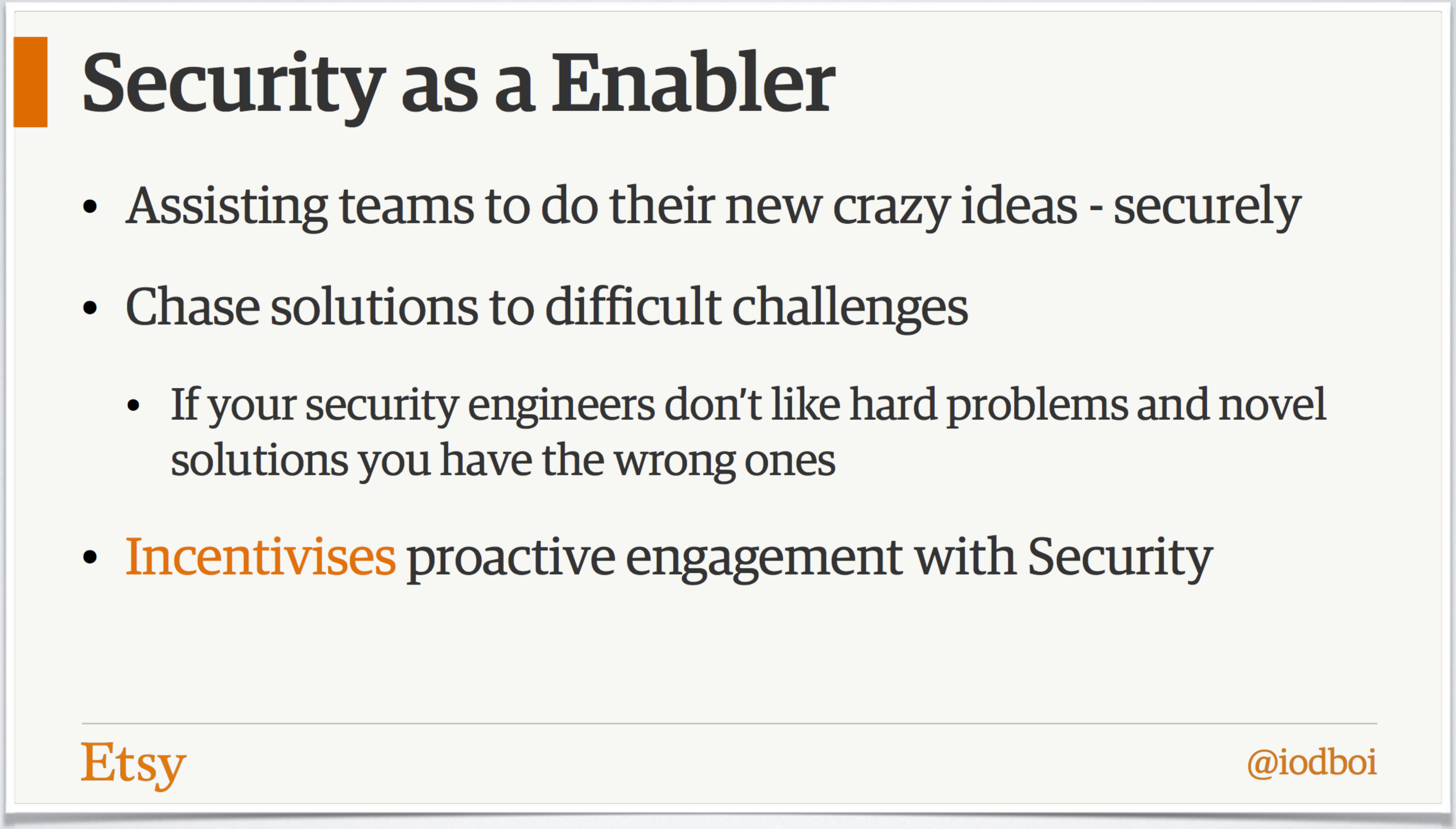
“network utopia”

“Want Complex, Need Simple”

thinkst
applied research

become super contrarian

thinkst
applied research



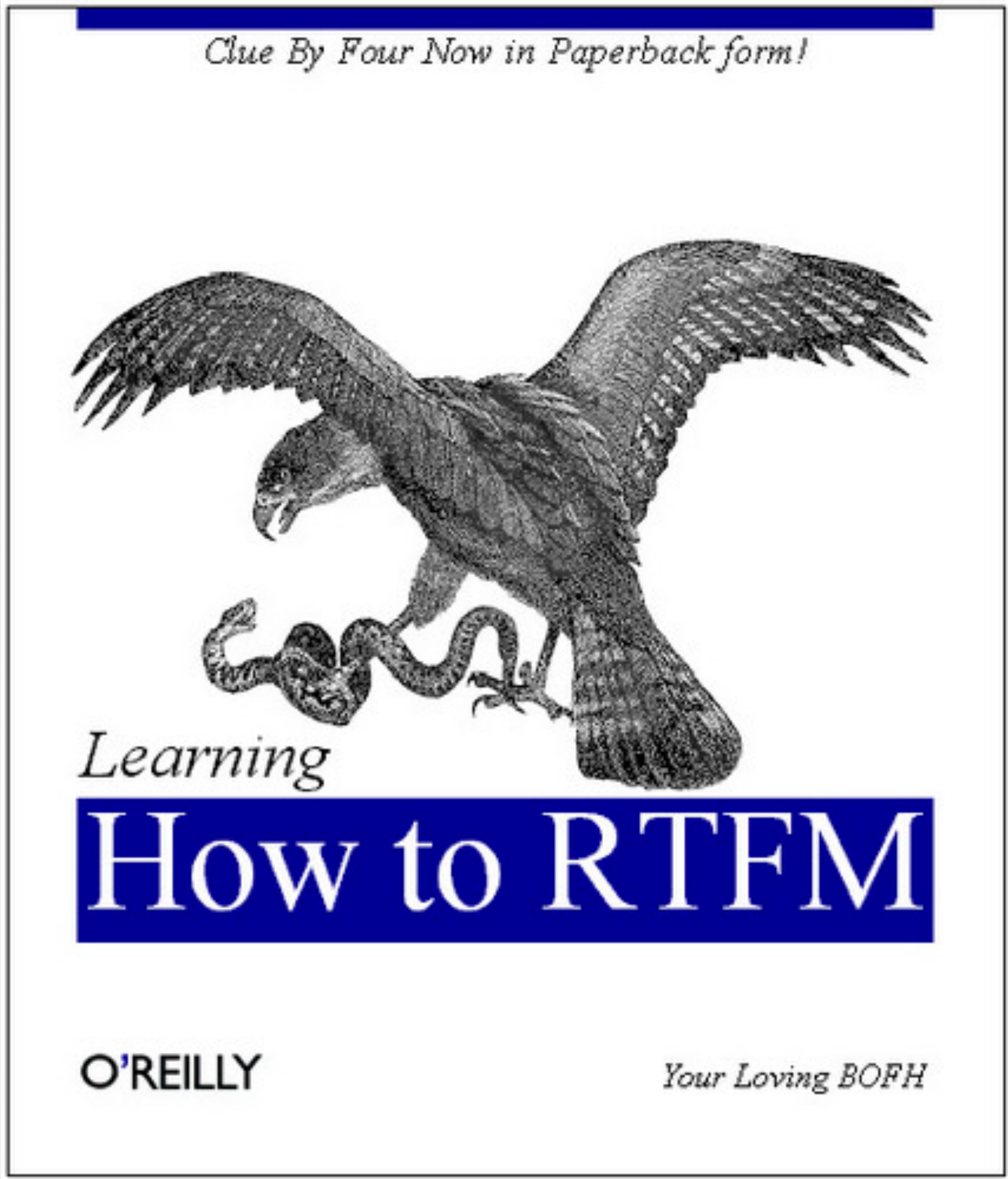
Security as a Enabler

- Assisting teams to do their new crazy ideas - securely
- Chase solutions to difficult challenges
  - If your security engineers don't like hard problems and novel solutions you have the wrong ones
- Incentivises proactive engagement with Security

Etsy

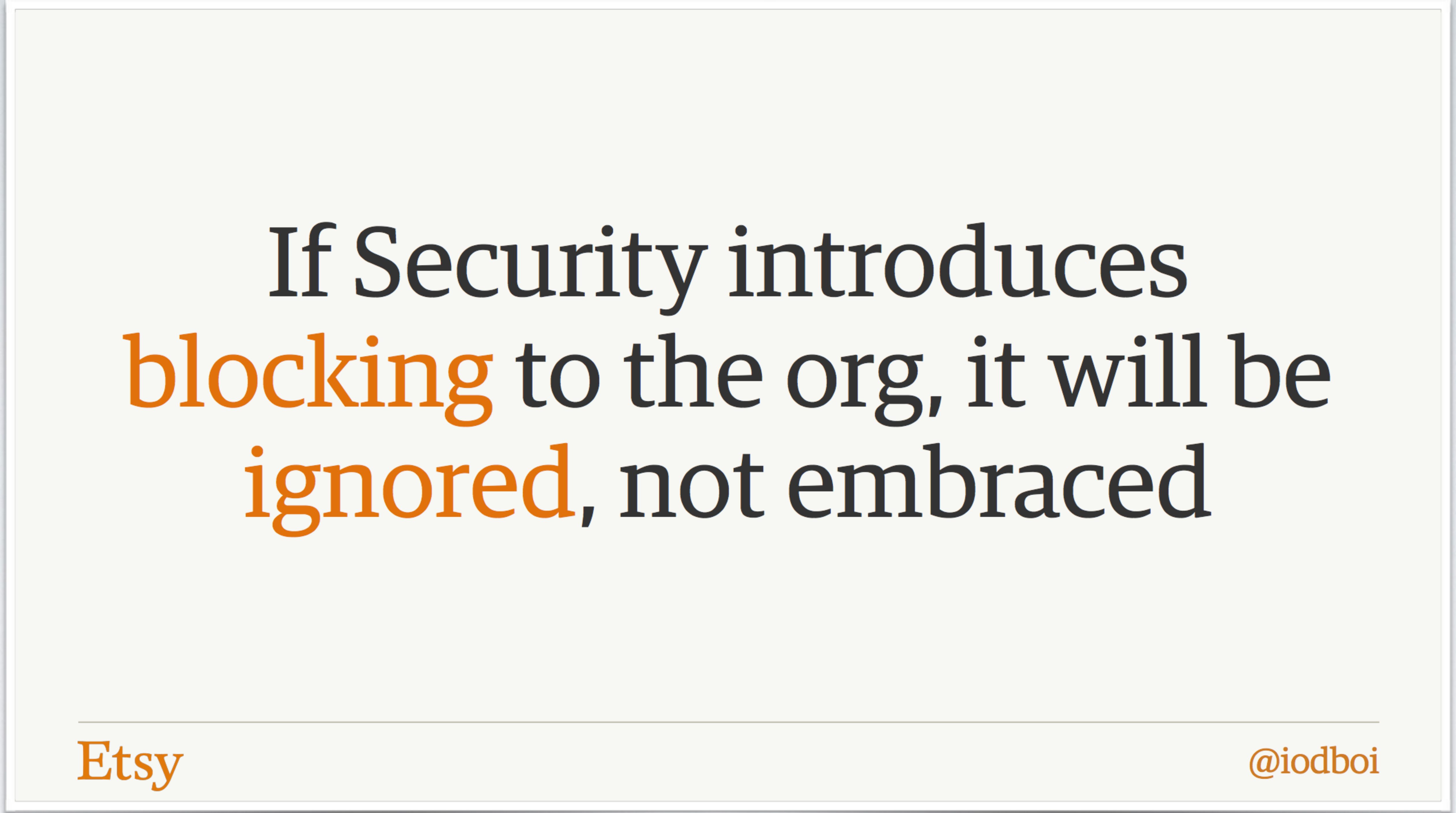
@iodboi

https://qconnewyork.com/system/files/presentation-slides/CraftingAnEffectiveSecurityOrg_QConNYC_RichSmith.pdf


Clue By Four Now in Paperback form!
Learning
How to RTFM
O'REILLY
Your Loving BOFH

Version 1.0
BASTARD OPERATOR FROM HELL
IN DISK SPACE, NOBODY CAN HEAR YOUR FILES SCREAM.

Bastard OPERATOR from hELL II
Son of the Bastard

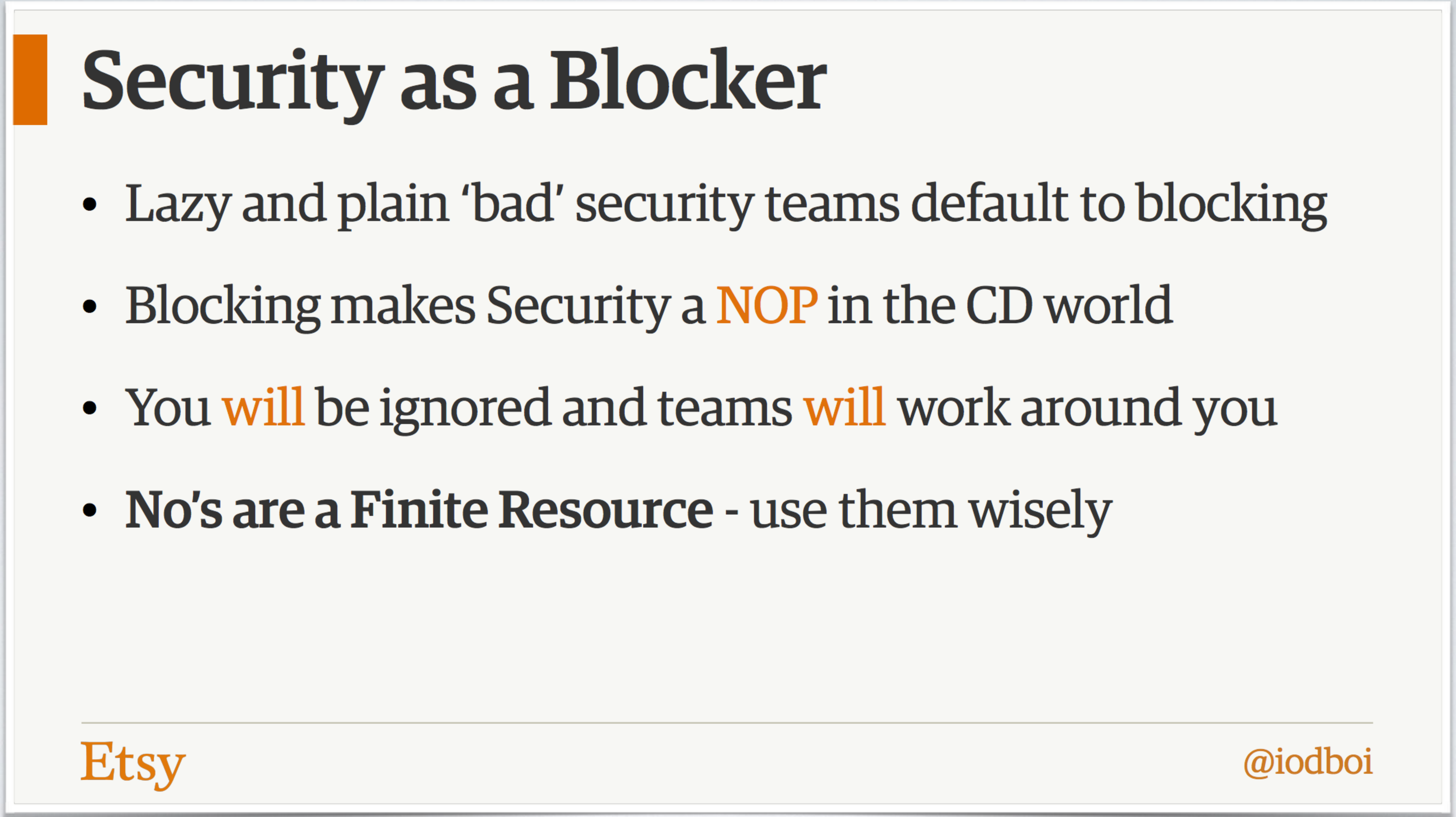


If Security introduces **blocking** to the org, it will be **ignored**, not embraced

Etsy

@iodboi

https://qconnewyork.com/system/files/presentation-slides/CraftingAnEffectiveSecurityOrg_QConNYC_RichSmith.pdf



Security as a Blocker

- Lazy and plain ‘bad’ security teams default to blocking
- Blocking makes Security a NOP in the CD world
- You will be ignored and teams will work around you
- **No’s are a Finite Resource** - use them wisely

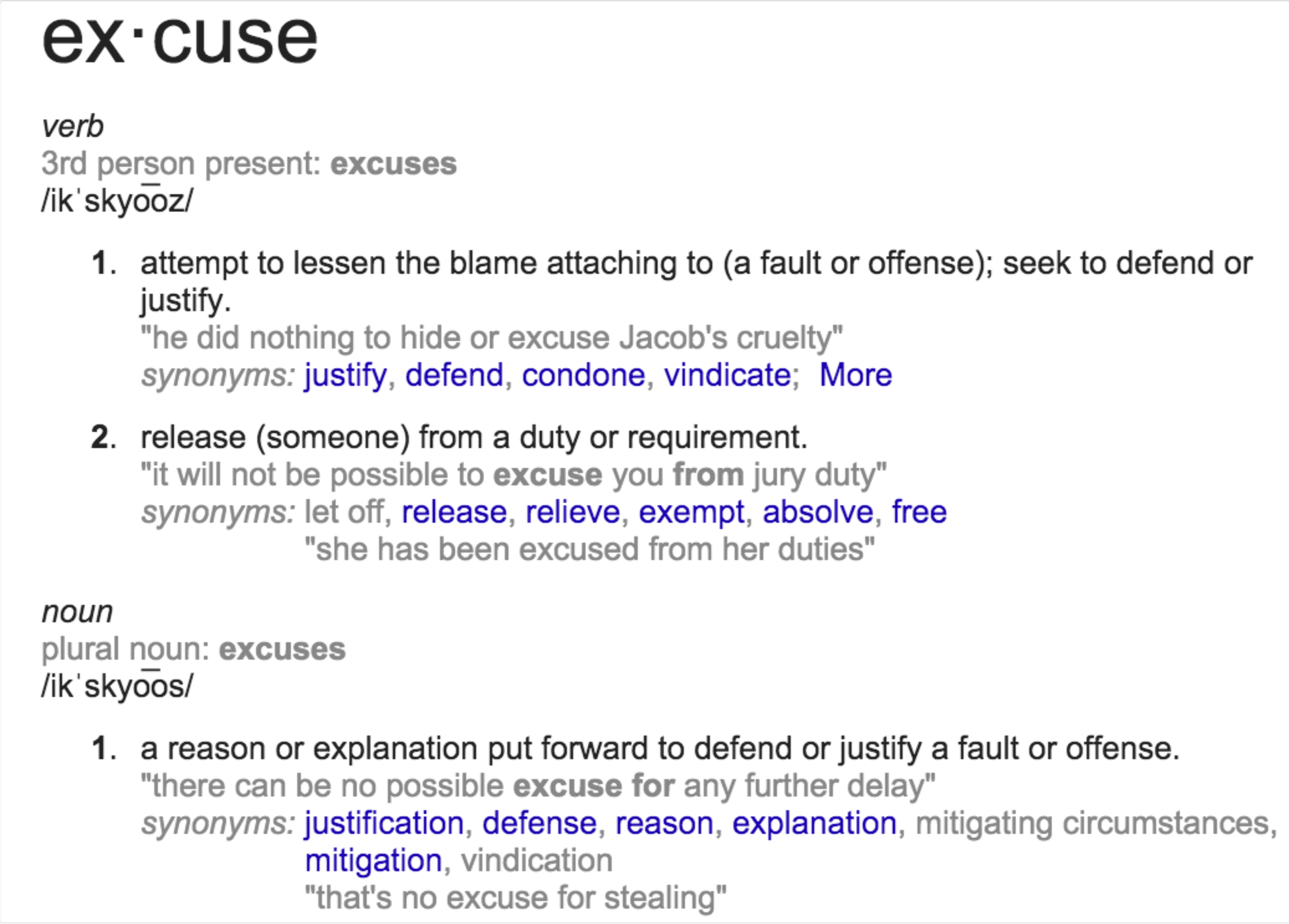
Etsy

@iodboi

https://qconnewyork.com/system/files/presentation-slides/CraftingAnEffectiveSecurityOrg_QConNYC_RichSmith.pdf

thinkst applied research

Enterprise obstacles



ex·cuse

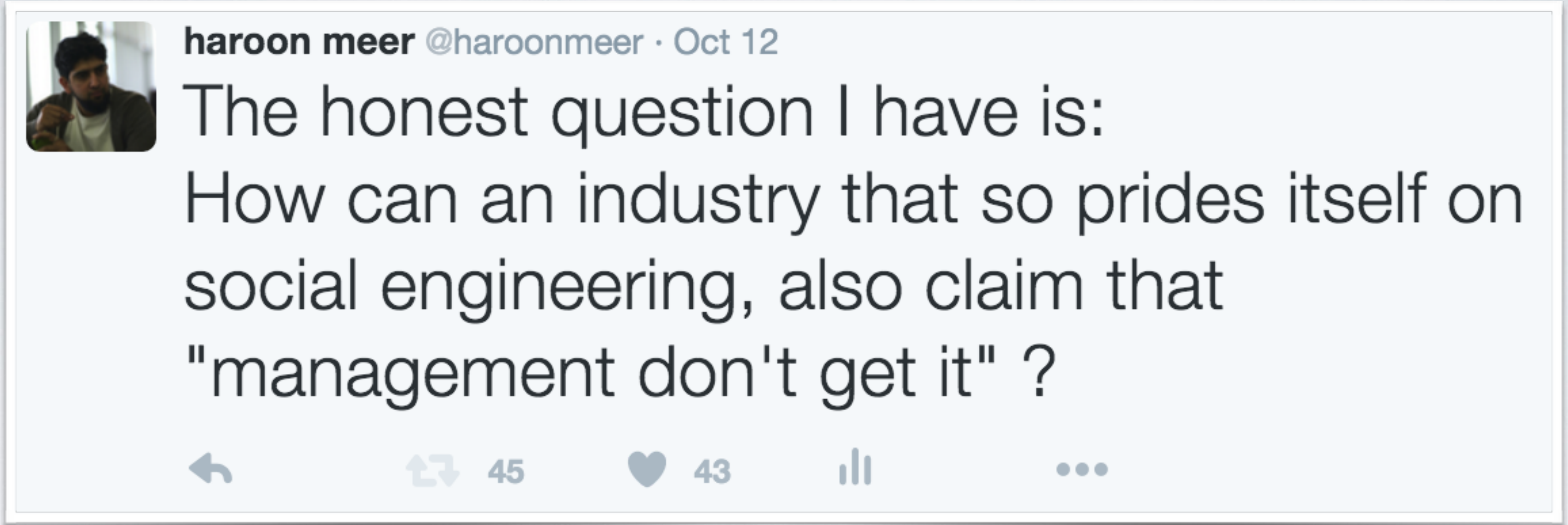
verb
3rd person present: **excuses**
/ikˈskyo͞oz/

1. attempt to lessen the blame attaching to (a fault or offense); seek to defend or justify.
   "he did nothing to hide or excuse Jacob's cruelty"
   synonyms: justify, defend, condone, vindicate; More

2. release (someone) from a duty or requirement.
   "it will not be possible to **excuse** you **from** jury duty"
   synonyms: let off, release, relieve, exempt, absolve, free
   "she has been excused from her duties"

noun
plural noun: **excuses**
/ikˈskyo͞os/

1. a reason or explanation put forward to defend or justify a fault or offense.
   "there can be no possible **excuse for** any further delay"
   synonyms: justification, defense, reason, explanation, mitigating circumstances, mitigation, vindication
   "that's no excuse for stealing"

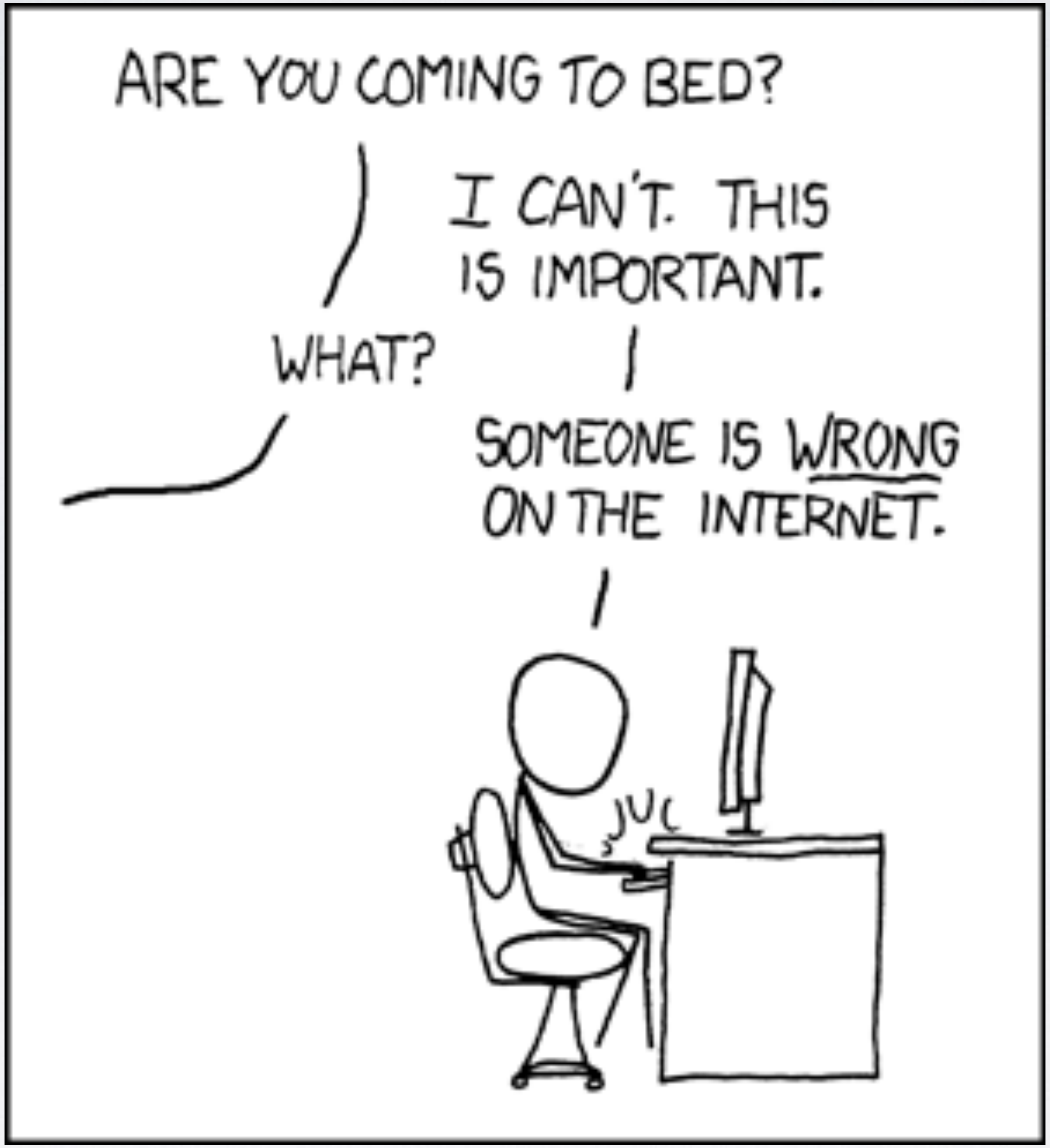


haroon meer @haroonmeer · Oct 12

The honest question I have is:
How can an industry that so prides itself on social engineering, also claim that "management don't get it" ?

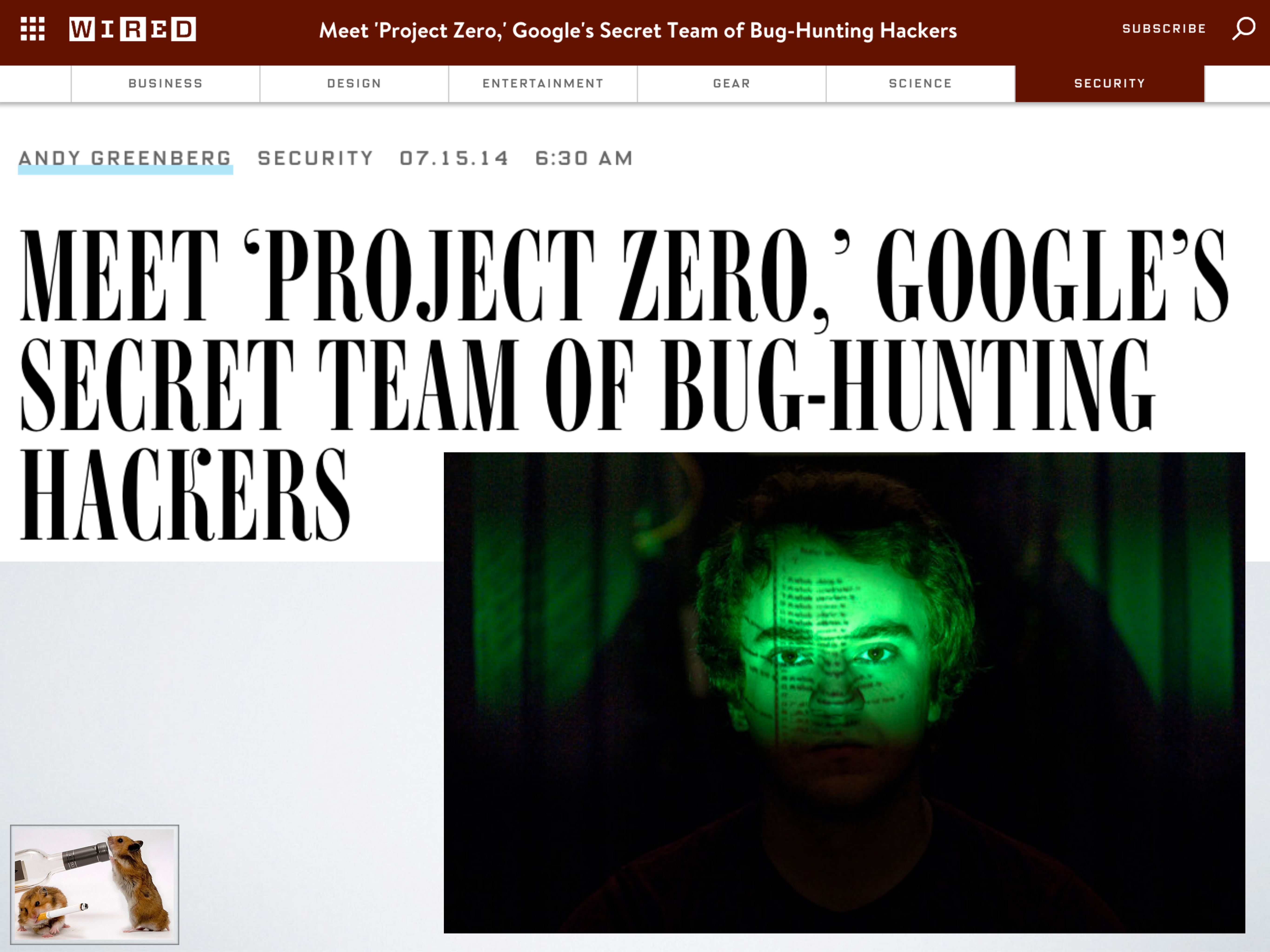
If I had a dollar for everytime I got distracted, I wish I had some ice cream.

Disclosure Debates


ARE YOU COMING TO BED?
I CAN'T. THIS IS IMPORTANT.
WHAT?
SOMEONE IS WRONG ON THE INTERNET.

https://xkcd.com/386/

thinkst applied research


WIRED
Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers
SUBSCRIBE
BUSINESS
DESIGN
ENTERTAINMENT
GEAR
SCIENCE
SECURITY

ANDY GREENBERG SECURITY 07.15.14 6:30 AM

MEET 'PROJECT ZERO,' GOOGLE'S SECRET TEAM OF BUG-HUNTING HACKERS

It would seem that most criticisms of eEye are not based on fact, but are rooted in a dislike of their brash style, in-your-face advisories, and choice of hair coloring.

http://www.securityfocus.com/news/238

thinkst applied research

focus on exploits / 0day

2 0-days away from the worst day of your life?

Golden Rule / 0-day rule

thinkst
applied research

“‘Conferences’”

thinkst
applied research

A Talk about Talks

thinkst
applied research

{haroon|marco}@thinkst.com

44CON 2013
HTTP://44CON.COM
@44CON

https://www.youtube.com/watch?v=BlVjdUkrSFY

thinkst
applied research

Chess Vs. Poker

Or: why we're playing the wrong game

Jacob Torrey

Cyber-security Philosopher and Boffin

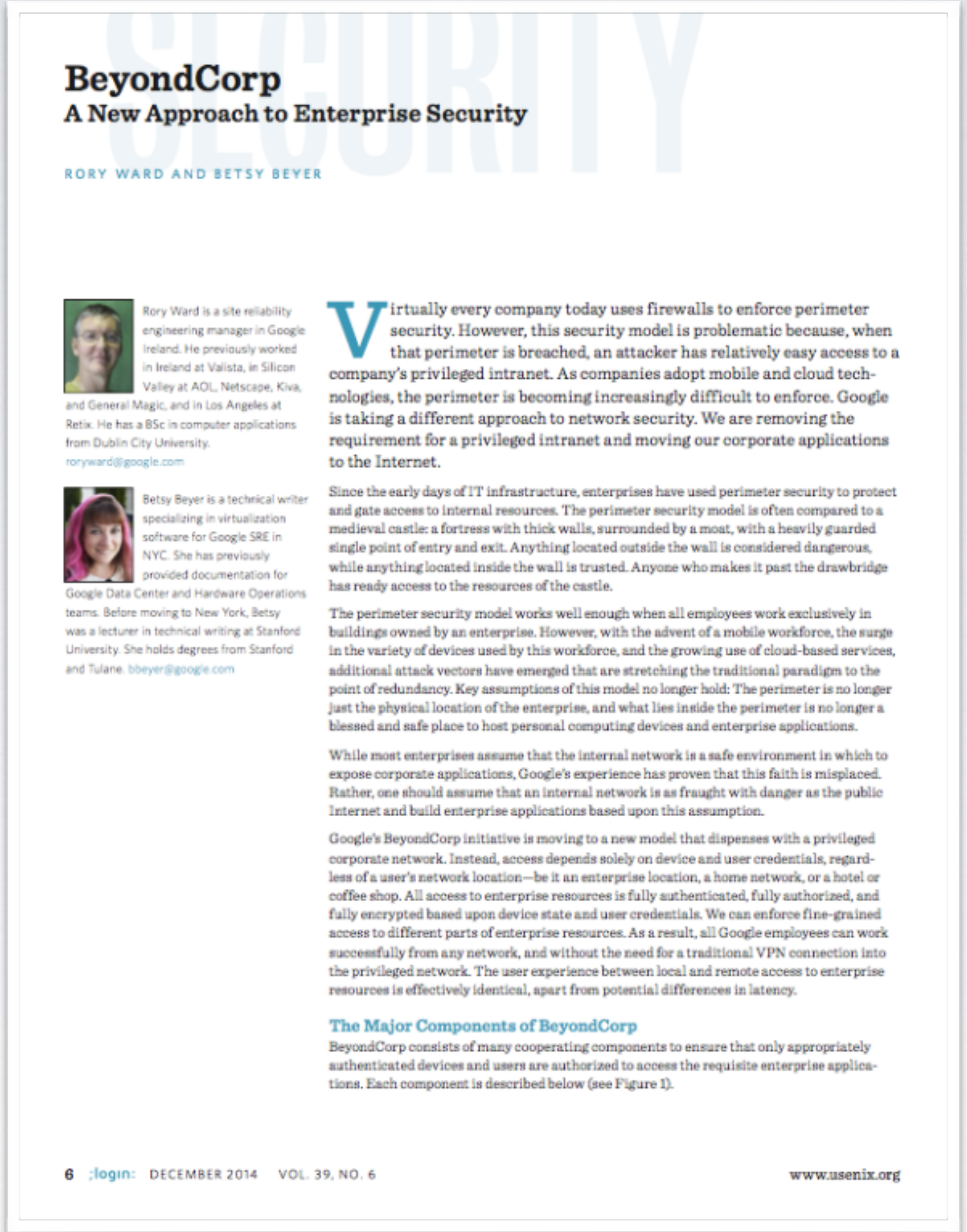
http://blog.jacobtorrey.com/chess-vs-poker

As the gap between the chess players and poker players grows, our contributions to the field become decreasingly relevant to the majority population of the Internet and we risk becoming a marginalized group, even though we are the most capable to help raise the bar for everyone

http://blog.jacobtorrey.com/chess-vs-poker

http://www.forbes.com/sites/thomasbrewster/
2015/09/16/airdrop-ios-vulnerability/

BeyondCorp



SECURITY

BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. roryward@google.com

Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

While most enterprises assume that the internal network is a safe environment in which to expose corporate applications, Google's experience has proven that this faith is misplaced. Rather, one should assume that an internal network is as fraught with danger as the public Internet and build enterprise applications based upon this assumption.

Google's BeyondCorp initiative is moving to a new model that dispenses with a privileged corporate network. Instead, access depends solely on device and user credentials, regardless of a user's network location—be it an enterprise location, a home network, or a hotel or coffee shop. All access to enterprise resources is fully authenticated, fully authorized, and fully encrypted based upon device state and user credentials. We can enforce fine-grained access to different parts of enterprise resources. As a result, all Google employees can work successfully from any network, and without the need for a traditional VPN connection into the privileged network. The user experience between local and remote access to enterprise resources is effectively identical, apart from potential differences in latency.

The Major Components of BeyondCorp

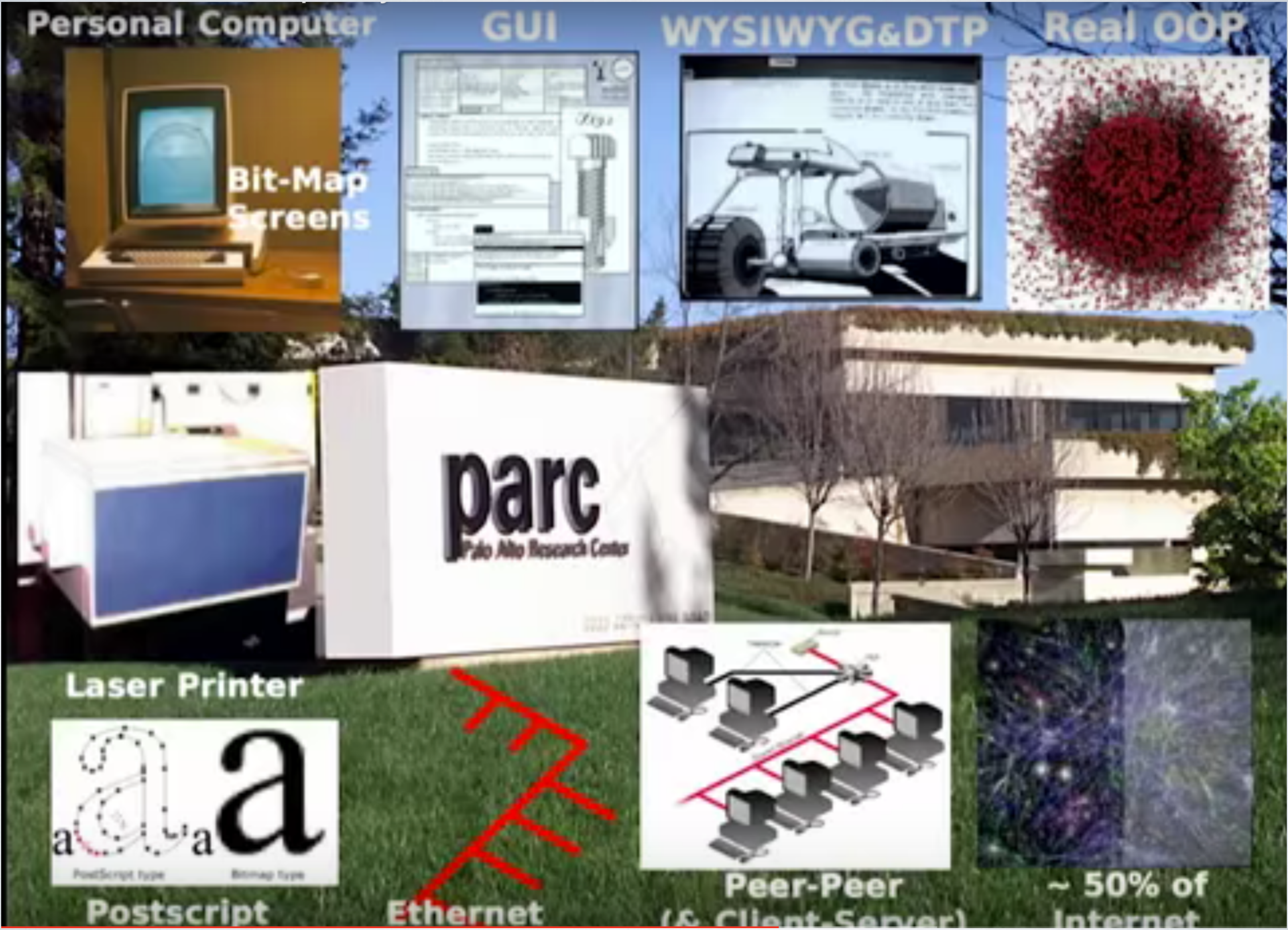
BeyondCorp consists of many cooperating components to ensure that only appropriately authenticated devices and users are authorized to access the requisite enterprise applications. Each component is described below (see Figure 1).

http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43231.pdf

“Researcher” count?

https://www.youtube.com/watch?v=NdSD07U5uBs

parc
Palo Alto Research Center



Personal Computer

GUI

WYSIWYG&DTP

Real OOP

Bit-Map Screens

Laser Printer

Postscript

Ethernet

Peer-Peer (& Client-Server)

~ 50% of Internet

Personal Computer

GUI

WYSIWYG&DTP

Real OOP

Bit-Map Screens

“9 1/2” Inventions

25 Researchers ~ 5 Years

~$12M/year in today's dollars

$30+ Trillion Dollars and counting

Laser Printer

Postscript

Ethernet

Peer-Peer (& Client-Server)

~ 50% of Internet

© AFP/GETTY IMAGES

□ Taken some wrong turns;

□ Developed some bad habits;

© AFP/GETTY IMAGES

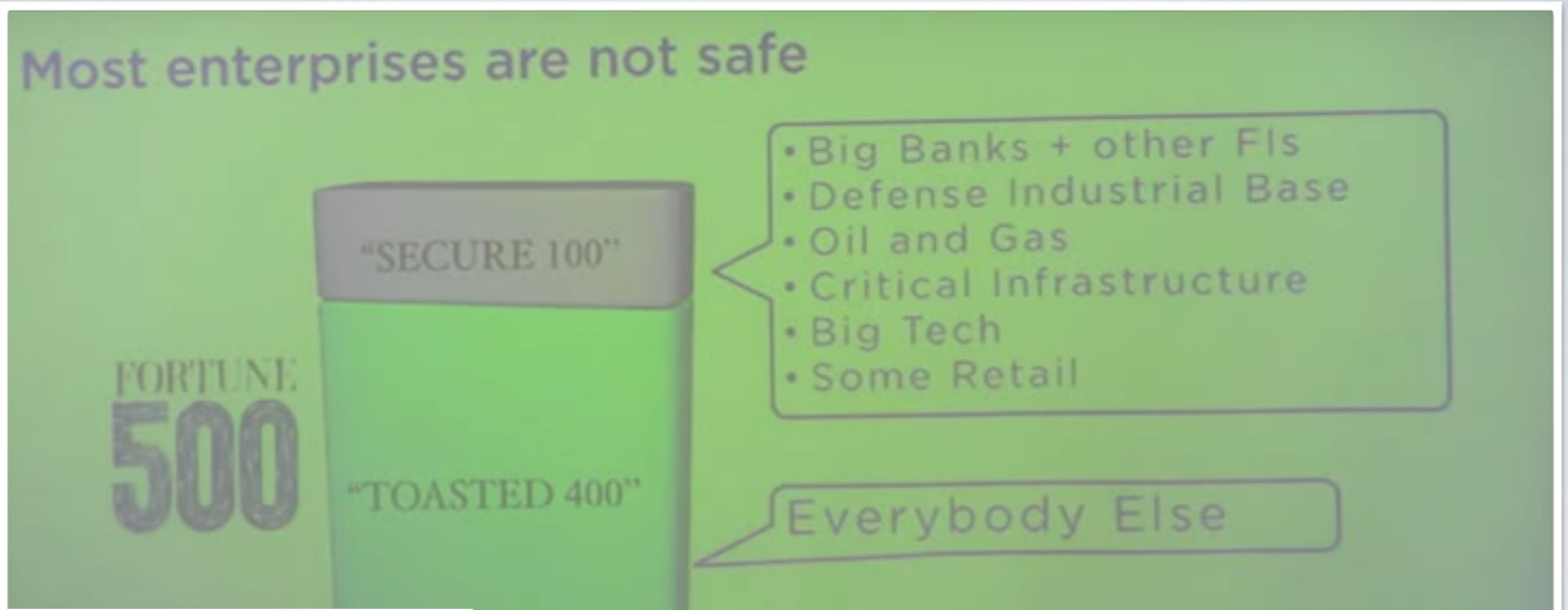
Missing some opportunities.

Re-examine old “‘truths’”

thinkst
applied research

Cheap Hacks Win

thinkst
applied research



Most enterprises are not safe

FORTUNE
500
"SECURE 100"
"TOASTED 400"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

Everybody Else

What are they missing?

- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

nobody owns the enterprise security problem

but it’s hard…

but it’s hard…

hard to go from “script.pl” to a shipping product..

but it’s hard…

hard to go from ‘‘always right consultant’’ to ‘‘vendor’’ but come on..

So.. in Summary

- We are at an important inflection point
- We simultaneously face a crisis of relevance and a crisis of confidence
- Our current trajectory leads to disaster

Step one is to simply acknowledge this

If you are a Defender

Make sure what you are aiming at matters;

No therapeutic difference

If you are an attacker

Realise that theres a bunch of interesting hacks waiting to be pulled off playing Defense!

If you are an Researcher

thinkst
applied research

We need you to show up and choose a side.

thinkst
applied research

throw your hat into the ring..

THANK YOU

thinkst
applied research

haroon@thinkst.com | @haroonmeer