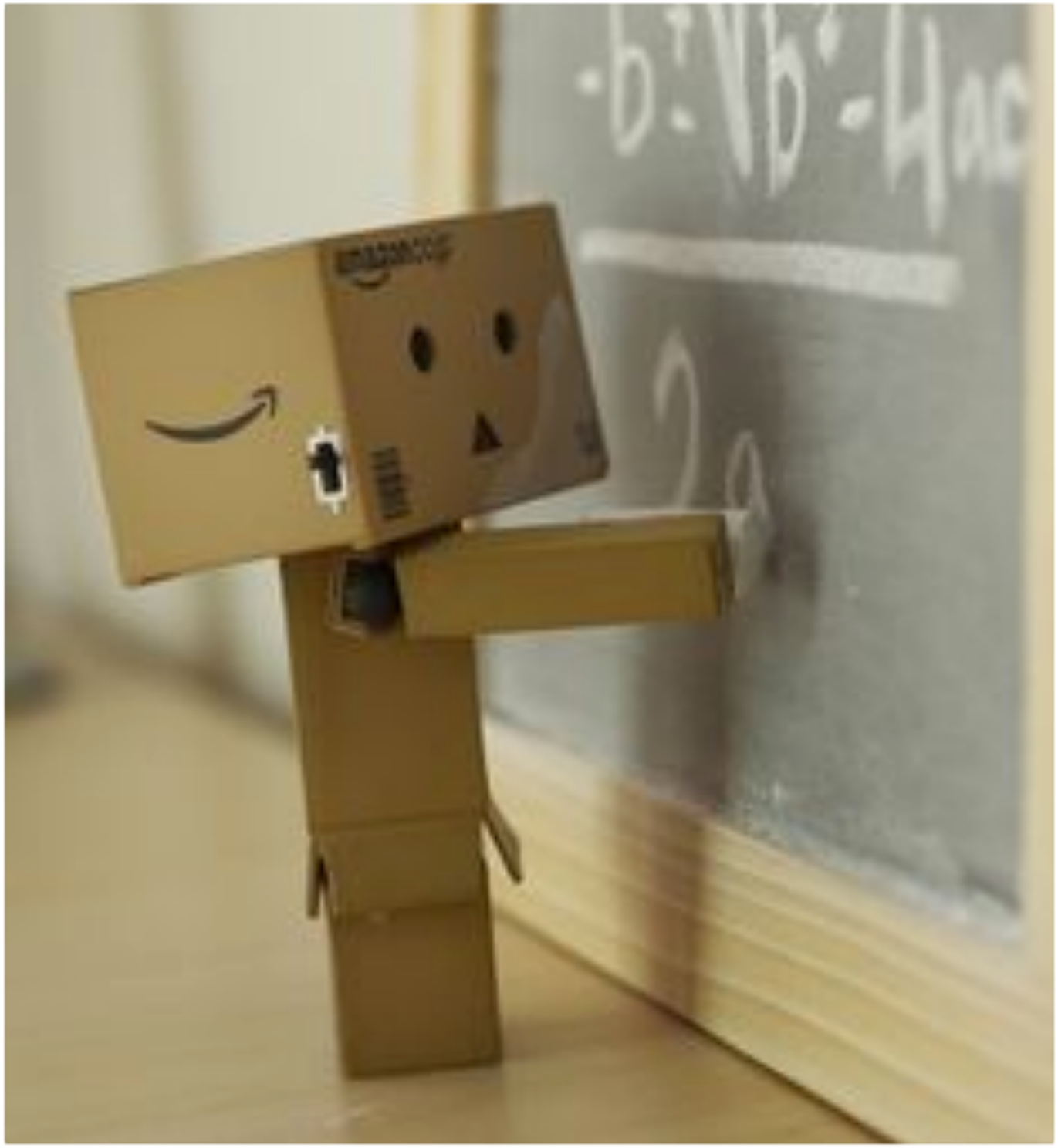


The 4-Minute Mile

haroon meer
Thinkst
@haroonmeer

Thanks!







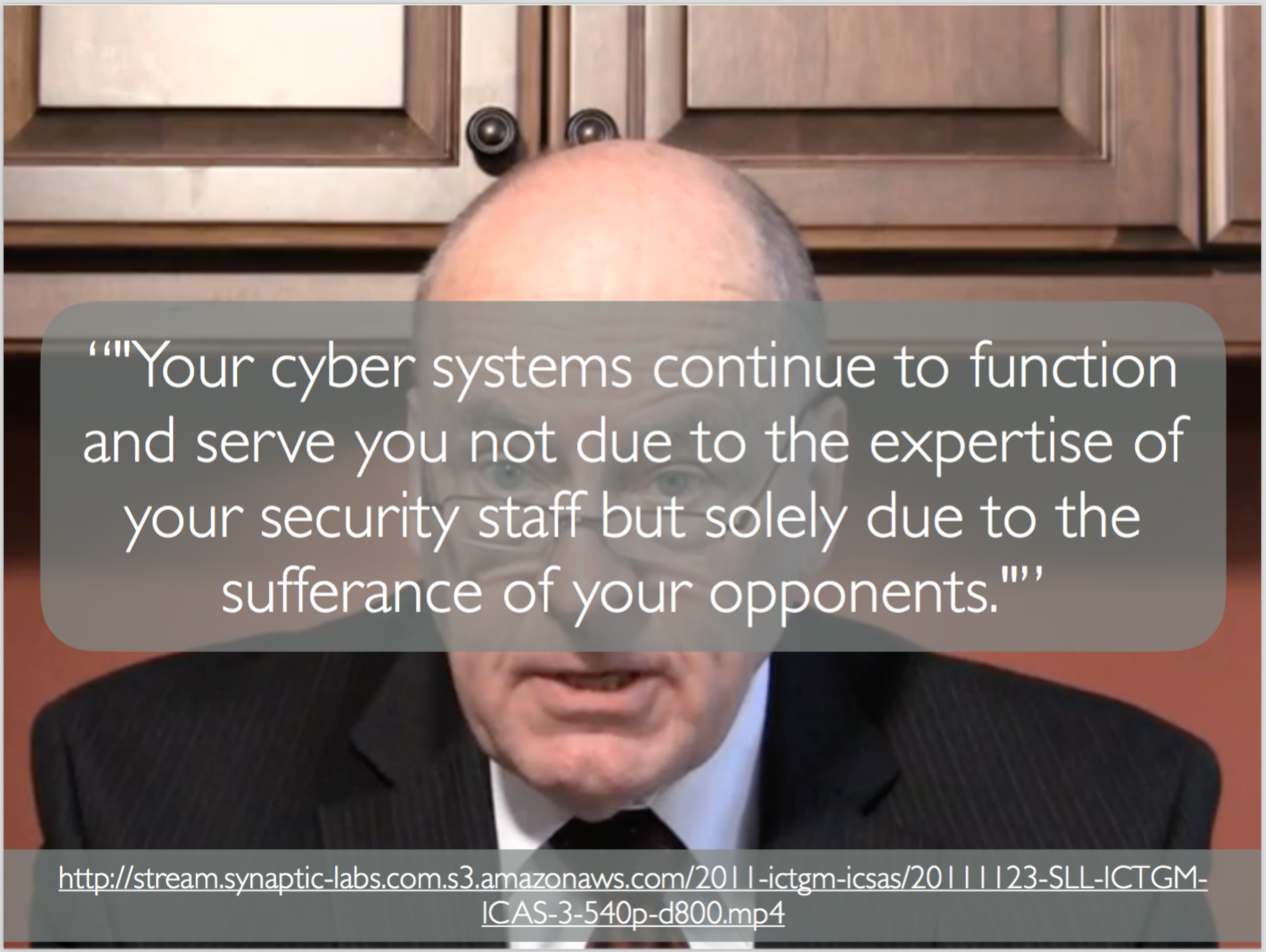
http://thinkst.com/resources/slides/itweb-2011-sb.pdf



http://thinkst.com/resources/slides/itweb-2011-sb.pdf



http://thinkst.com/resources/slides/itweb-2011-sb.pdf

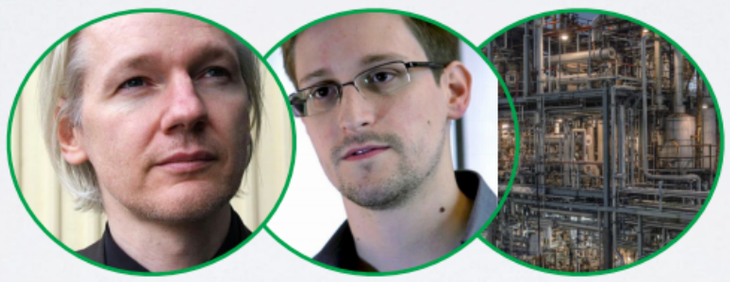


http://stream.synaptic-labs.com.s3.amazonaws.com/2011-ictgm-icsas/20111123-SLL-ICTGM-ICAS-3-540p-d800.mp4





Why?



https://vimeo.com/147743404

Why?





https://vimeo.com/147743404






HITACHI
Warning:
Do not remove
the battery.
Avertissement :
ne pas retirer
la batterie.
Achtung:
Entfernen Sie die
Batterie nicht.


16GB
micro SD

But..




DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY


Verizon
65%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel



10 Immutable Laws of Security

Archived content. No warranty is made as to technical accuracy. Content may contain URLs that were valid when originally published, but now link to sites or pages that no longer exist.

Here at the Microsoft Security Response Center, we investigate thousands of security reports every year. In some cases, we find that a report describes a bona fide security vulnerability resulting from a flaw in one of our products; when this happens, we develop a patch as quickly as possible to correct the error. (See "A Tour of the Microsoft Security Response Center"). In other cases, the reported problems simply result from a mistake someone made in using the product. But many fall in between. They discuss real security problems, but the problems don't result from product flaws. Over the years, we've developed a list of issues like these, that we call the 10 Immutable Laws of Security.

Don't hold your breath waiting for a patch that will protect you from the issues we'll discuss below. It isn't possible for Microsoft—or any software vendor—to "fix" them, because they result from the way computers work. But don't abandon all hope yet—sound judgment is the key to protecting yourself against these issues, and if you keep them in mind, you can significantly improve the security of your systems.

On This Page

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more
Law #5: Weak passwords trump strong security
Law #6: A computer is only as secure as the administrator is trustworthy
Law #7: Encrypted data is only as secure as the decryption key
Law #8: An out of date virus scanner is only marginally better than no virus scanner at all
Law #9: Absolute anonymity isn't practical, in real life or on the Web
Law #10: Technology is not a panacea

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY


Verizon
65%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel



Security TechCenter

Search TechNet with Bing

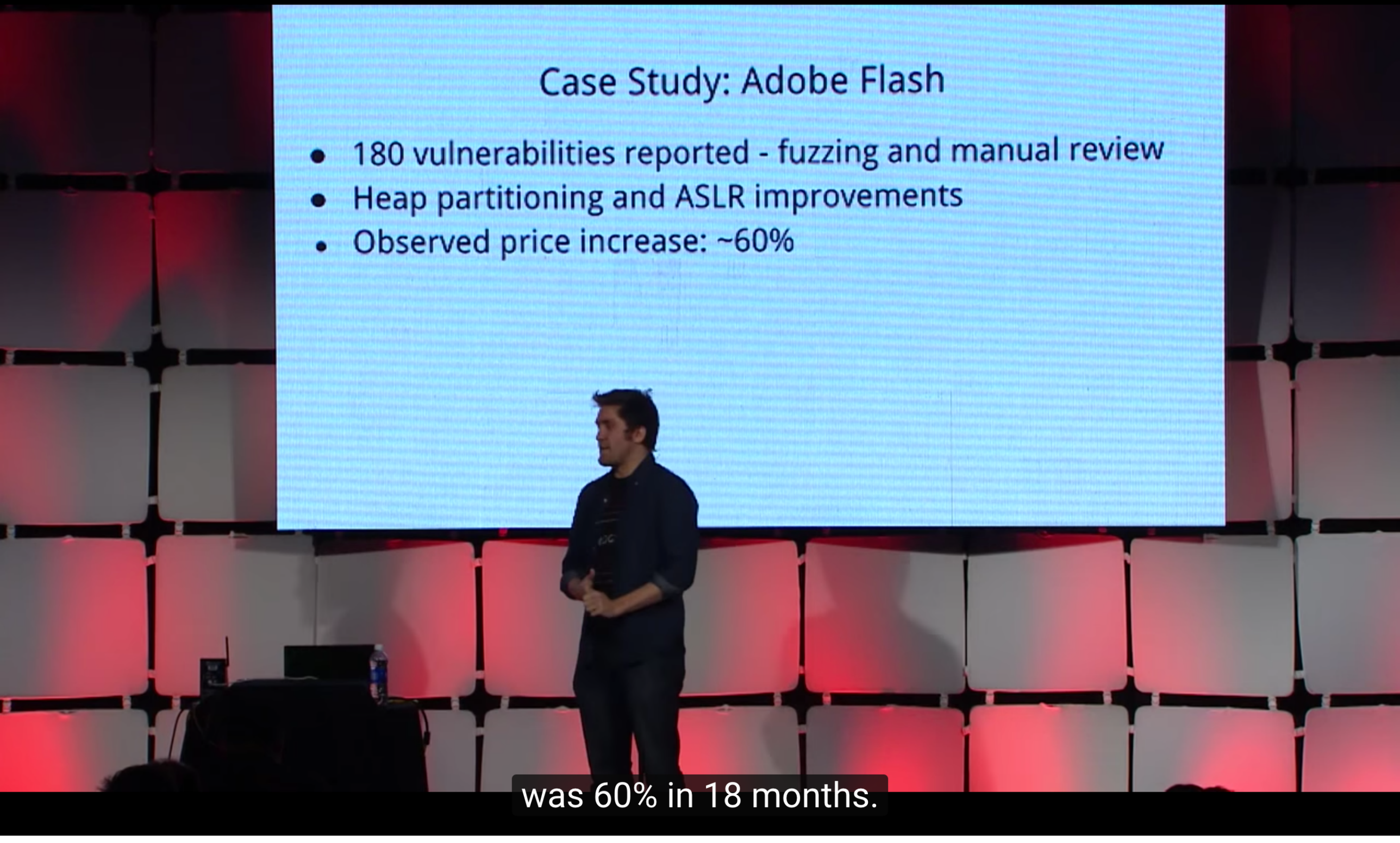
Home | Security Updates | Tools | Learn | Library | Support

RESPONSE | BULLETINS | ADVISORIES | MYBULLETINS

Mitigation Bypass and Bounty for Defense Terms

PROGRAM DESCRIPTION

Microsoft is pleased to announce the launch of the Microsoft Mitigation Bypass Bounty and Bounty for Defense Program beginning June 26, 2013. Through this program, individuals across the globe have the opportunity to submit a novel mitigation bypass against our latest Windows platform, and are also invited to submit a defense idea that would block an exploitation technique that currently bypasses the latest platform mitigations. Under this program, qualified mitigation bypass submissions are eligible for payment of up to $100,000 USD and qualified defensive techniques are eligible for a bounty of up to $100,000, for a total of up to $200,000 USD. All bounties will be paid out at Microsoft's discretion.



https://www.youtube.com/watch?v=ZKIIPu1wqHs




amazon.co.jp



Most enterprises are not safe



Most enterprises are not safe



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

Most enterprises are not safe



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

Everybody Else

FORTUNE

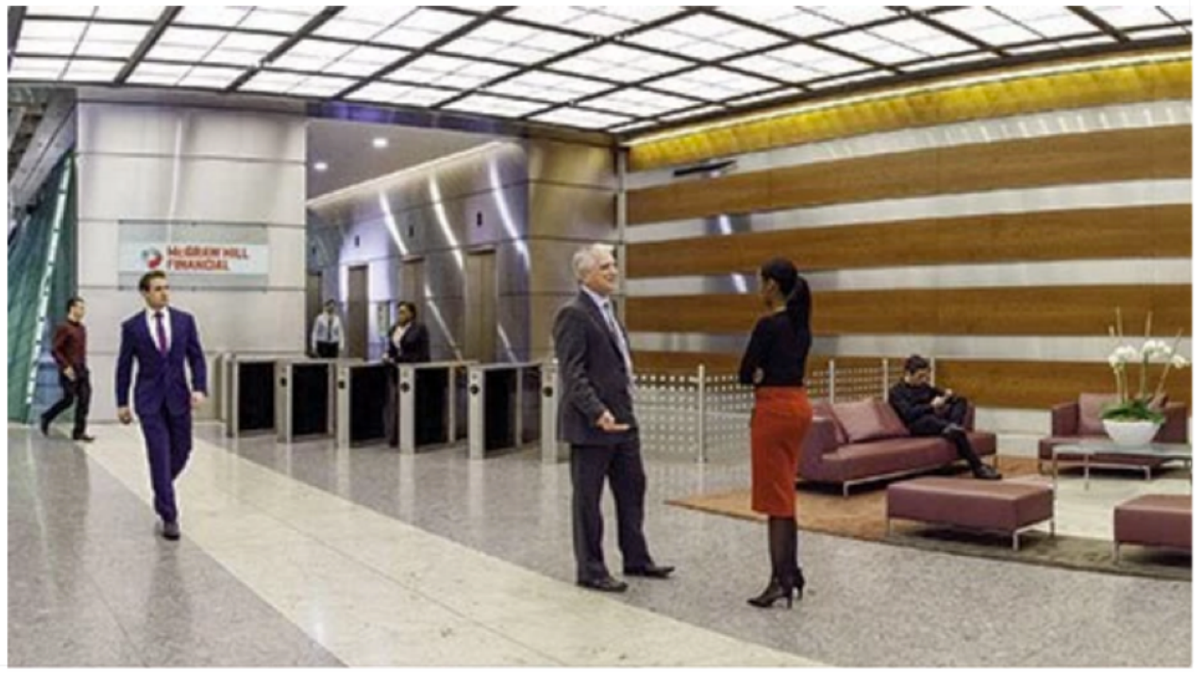
FORTUNE 500 2015

500. McGraw Hill Financial

LAST YEAR'S RANK: 484 ↓

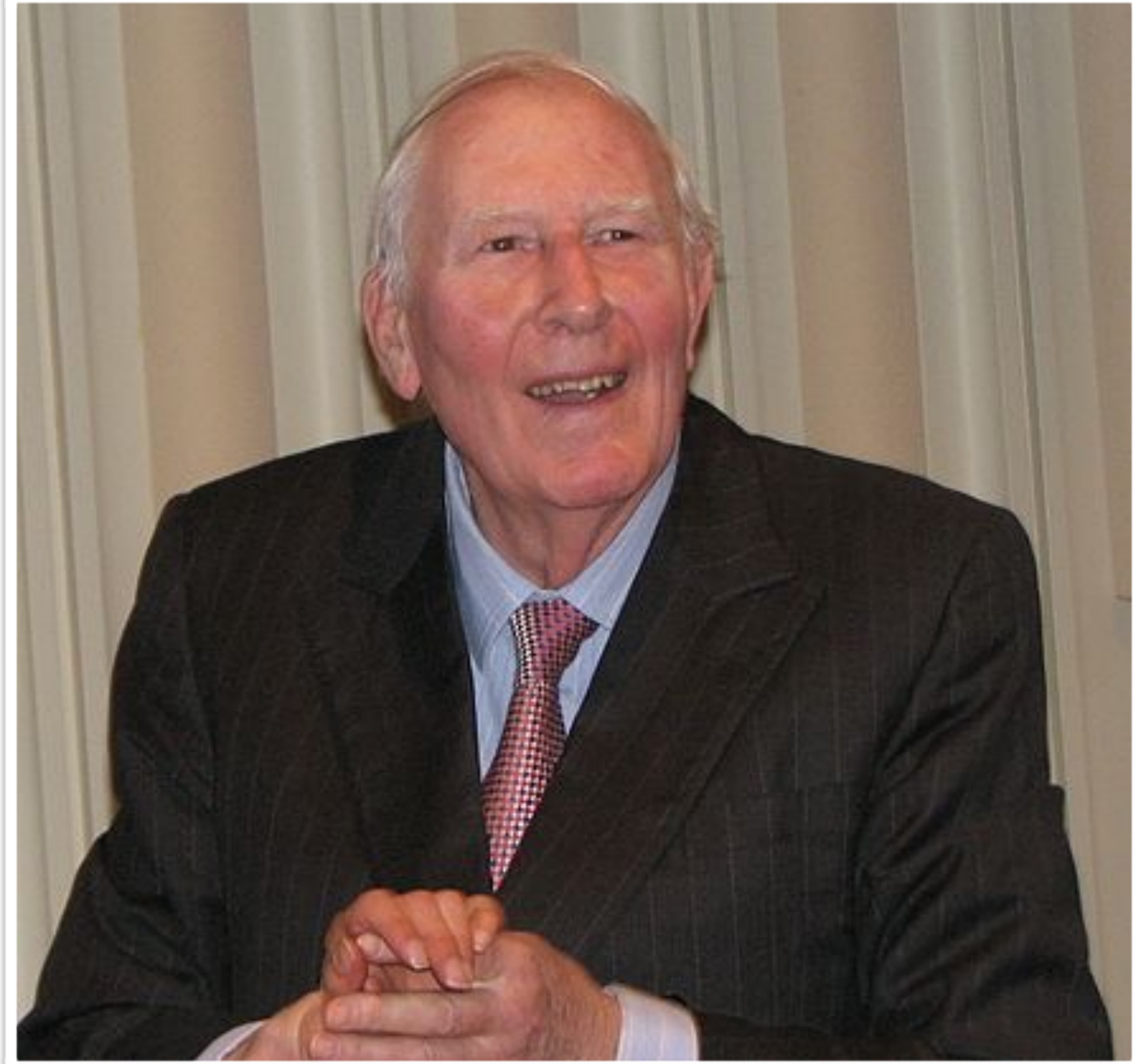
Prev Company | Next Company

The New York-based firm sells financial information and analytics through brands like Standard & Poor's ratings, S&P Dow Jones Indices, and J.D. Power.



Market Value (as of March 31, 2015) - ~USD 28 Billion








2
5
4


amazon.co.jp

1) Why are we failing?

2) Is anyone succeeding?

So why can’t we (currently) secure our companies ?

there are lots of reasons

there are lots of reasons

(and that becomes part of the problem)


amazon.co.jp
amazon.co.jp

Generic Solutions Fail



haroon meer
@haroonmeer

FireEye exists to stop 0days. Raft of 0days reported in FireEye boxes.

Obviously we need another box that stops 0days in front of FE boxes.

RETWEETS 219 LIKES 130



11:26 AM - 8 Sep 2015

iWeb events
thinkst applied research



Dino A. Dai Zovi
@dinodaizovi

Following

Security anti-pattern #34: Attempting to mitigate vulnerable attack surfaces with higher-privileged *and more vulnerable* attack surfaces.

RETWEETS 46 LIKES 57



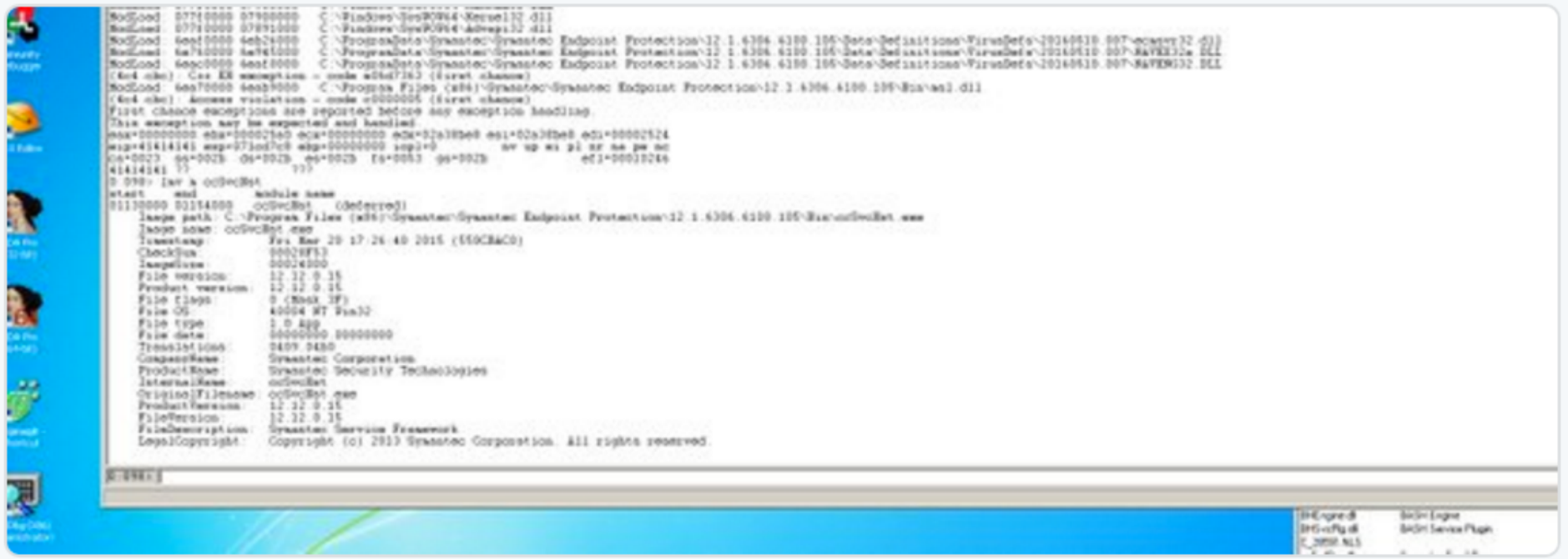
9:13 PM - 16 Apr 2016

https://twitter.com/dinodaizovi/status/721416219799097344



Tavis Ormandy @taviso · May 11

Many remote stack overflows in Symantec Endpoint. No big deal, because /GS is the default since 2005, right? Hahaha.



340 249

https://twitter.com/taviso/status/730249521247068162

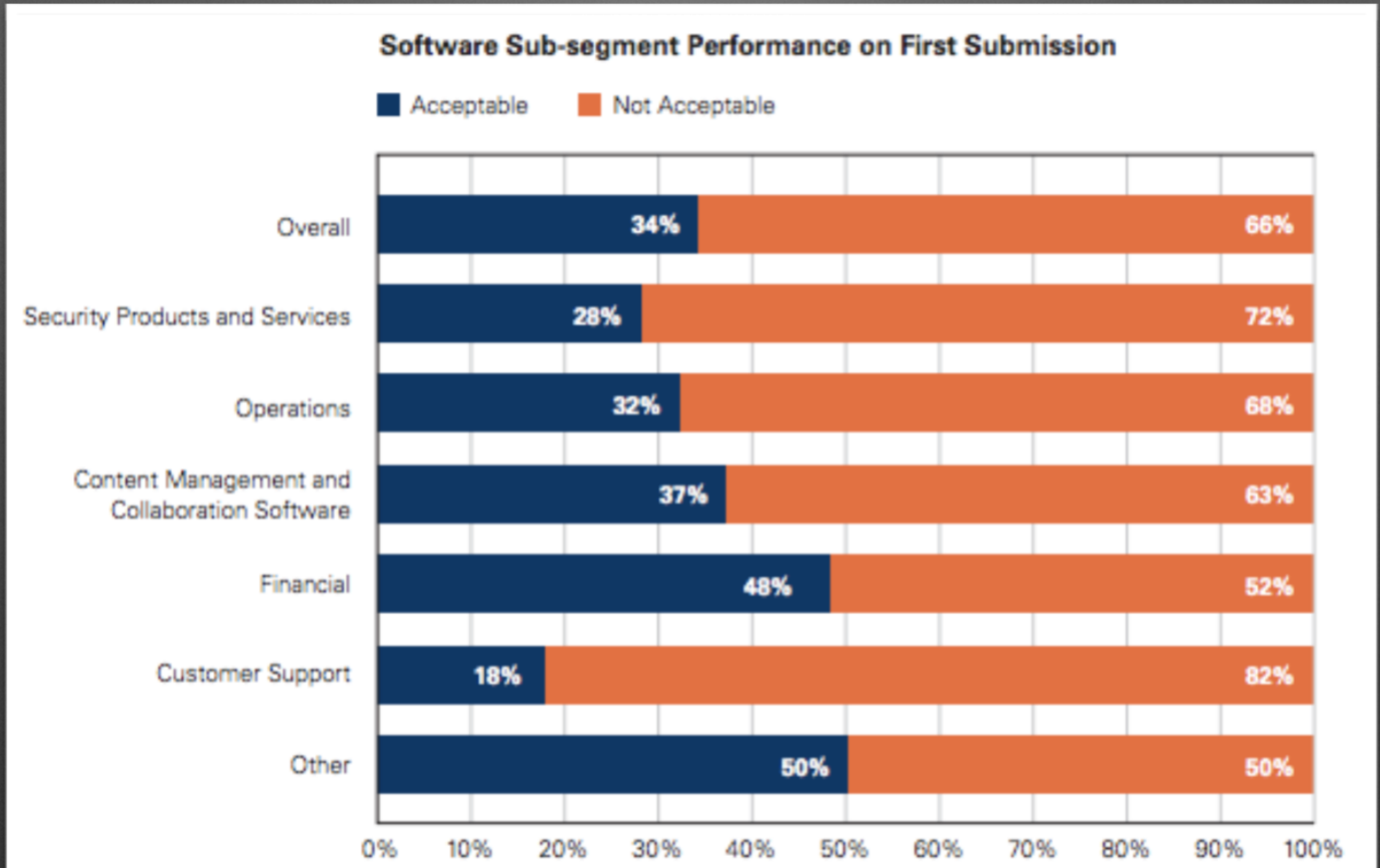


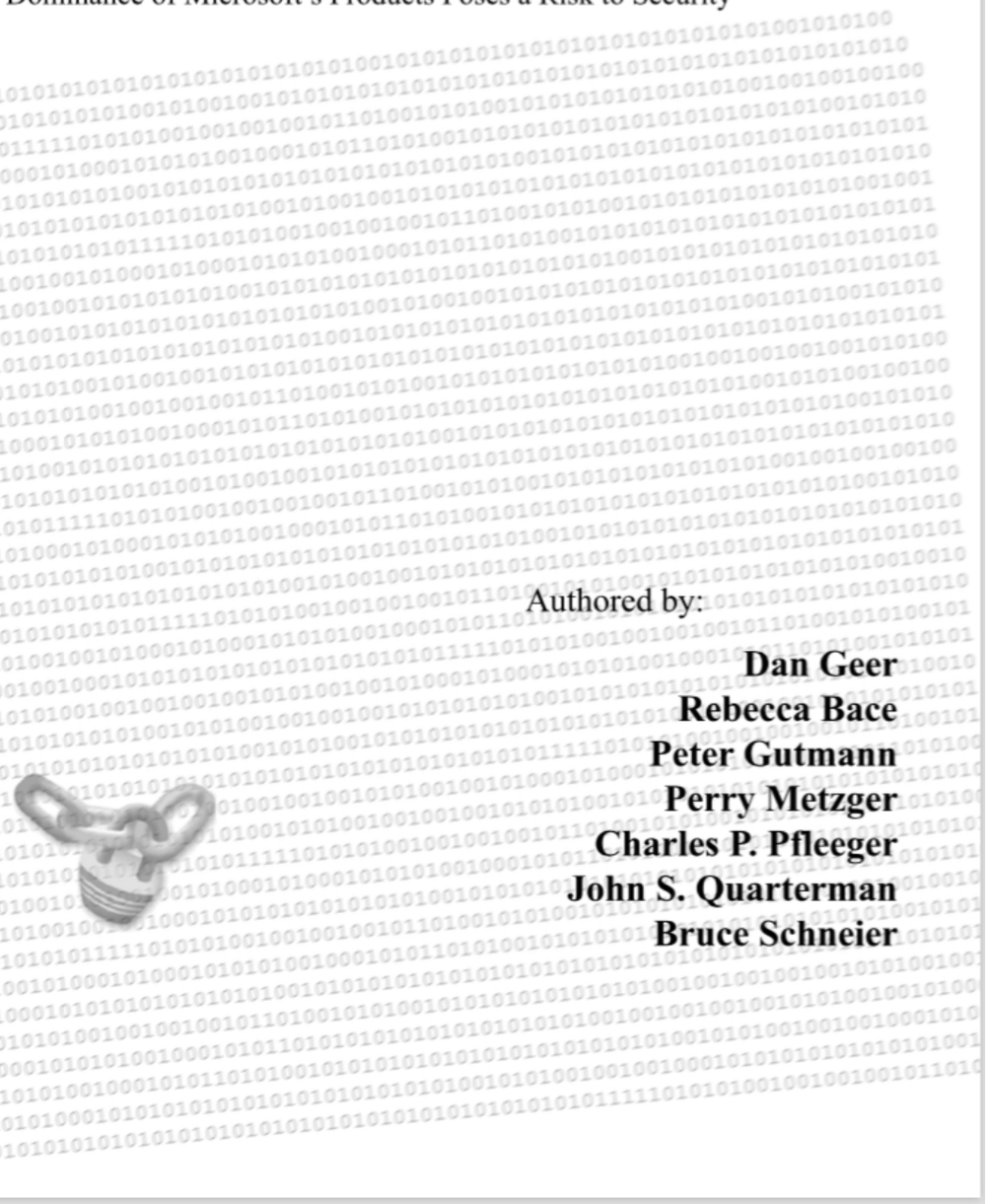
Figure 28: Software Sub-segment Performance on First Submission

https://info.veracode.com/state-of-software-security-report-volume3.html

http://web.stanford.edu/class/msande91si/www-spr04/readings/week4/cyberinsecurity.pdf

Cyber*In*security: The Cost of Monopoly

How the Dominance of Microsoft's Products Poses a Risk to Security



Authored by:

Dan Geer
Rebecca Bace
Peter Gutmann
Perry Metzger
Charles P. Pfleeger
John S. Quarterman
Bruce Schneier

“most popular box solutions are useless against attackers”

alex stamos - yahoo

“we used to be a huge fire eye customer, we’re ripping them all out”

alex stamos - yahoo

Contrarian Opinion Ahead

Good Defense is a series of “internal hacks”

we've been told not to go for the "quick hacks".

..that solutions needed to be enterprise'y & come in a shiny box (or at least have an SLA)



things move too fast


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

ok solutions that work today

>

perfect solutions that might work tomorrow

egg-samples



Who's a Domain Admin?



CanaryTokens

http://canarytokens.org/



SSH Source-IP?



there's just one thing

that stops you…


PEOPLE
PROCESS
TECHNOLOGY


SOCIAL BUSINESS
TECHNOLOGY
ORGANIZATIONAL READINESS
SOCIAL BRAND


TECHNOLOGY
PEOPLE
PROCESS


PROCESS
PEOPLE
SERVICES OPERATIONS COMPETENCY
TECHNOLOGY


People
Technology
Process


TECHNOLOGY


PEOPLE
Staff Training & Awareness
Professional Skills and Qualifications
Competent Resources
PROCESS
Management Systems
Governance Frameworks
Best Practice
IT Audit
TECHNOLOGY
You can't deploy technology without competent people, support processes or an overall plan.


PEOPLE
Business Process Understanding
Segregation & Controls
Key Performance Measurement
System Implementation
System Evaluation & Selection
System Audit & Review
Business Process Re-engineering
Policies, Procedures & Reporting
Roles & Responsibilities
PROCESS
TECHNOLOGY


Strategy
People
Technology
Process
Compliance
Project Management
Change Management

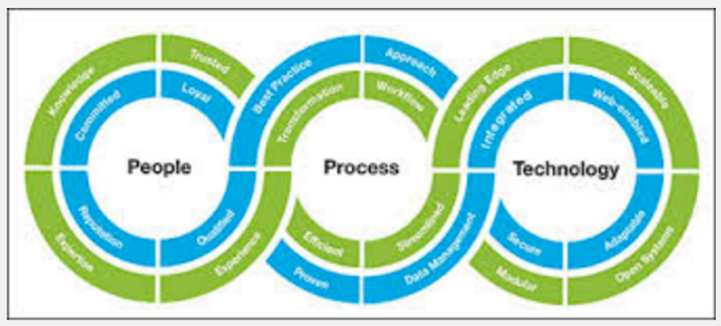

Continuous Improvement
People
Process
Technology
Innovation
Innovation
Continuous Improvement


Process
Success
People
Technology

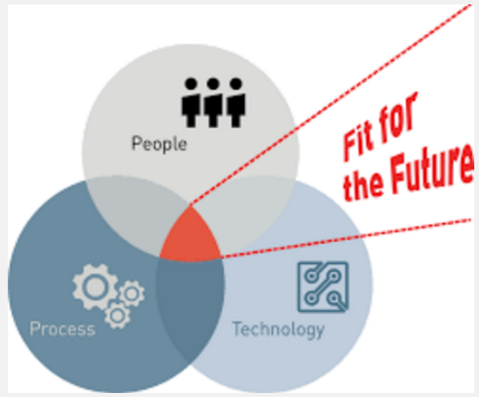

PROCESS
PEOPLE
SUCCESS
TECHNOLOGY

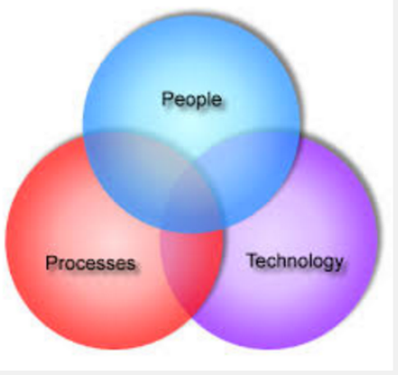

Process
Technology
People


People
Process
Technology

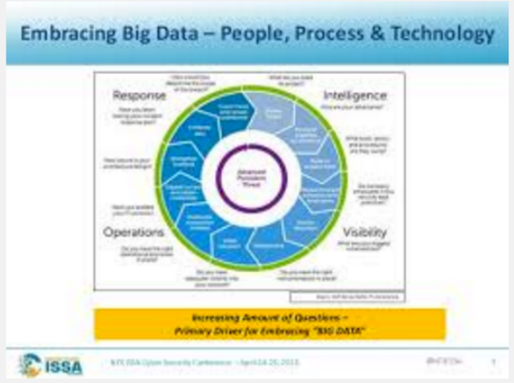

People
Process
Technology
Knowledge
Committed
Trusted
Loyal
Best Practice
Transformation
Approach
Workflow
Leading Edge
Integrated
Scalable
Web-enabled
Perception
Expertise
Quality
Experience
Efficient
Proven
Streamlined
Data Management
Secure
Modular
Adaptable
Open Systems


People
Strategy
Process
Technology


People
Fit for the Future
Process
Technology


People
Processes
Technology


• Reallocate of tasks
• Extend Training to Supplier
• Organization Change
People
Process
Technology
• Align tasks to milestones
• Re-define work flow
• Standardise library nomenclature
• Rework security matrix
• Activate vendor Portal
• Create task dependencies

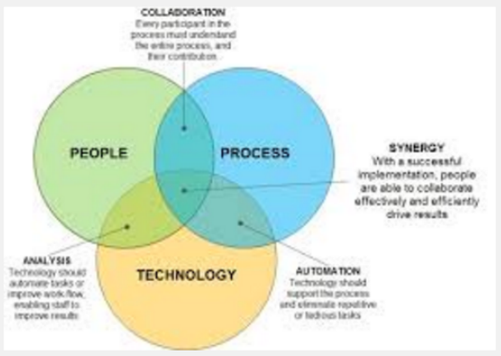

Embracing Big Data – People, Process & Technology
Response
Intelligence
Operations
Visibility
Increasing Amount of Questions –
Primary Driver for Embracing "BIG DATA"
ISSA


Process
People
Technology


MONITORING
TROUBLE-SHOOTING
PEOPLE
TECHNOLOGY
PROCESS
IMPROVEMENT
REMEDIATION


firehost
People, Process, & Technology
PEOPLE
PROCESS
TECHNOLOGY


People
Process
Technology


COLLABORATION
PEOPLE
PROCESS
SYNERGY
With a successful implementation, people are able to collaborate effectively and efficiently drive results
ANALYSIS
AUTOMATION
TECHNOLOGY




PEOPLE
PROCESS
TECHNOLOGY


PEOPLE
PROCESS
TECHNOLOGY


SOCIAL BUSINESS
TECHNOLOGY
ORGANIZATIONAL READINESS
SOCIAL BRAND


TECHNOLOGY
PEOPLE
PROCESS


PROCESS
PEOPLE
SERVICES OPERATIONS COMPETENCY
TECHNOLOGY


People
Technology
Process


PROCESS
TECHNOLOGY


PEOPLE
Staff Training & Awareness
Professional Skills and Qualifications
Competent Resources
PROCESS
Management Systems
Governance Frameworks
Best Practice
IT Audit
TECHNOLOGY
You can't deploy technology without competent people, support processes or an overall plan.


PEOPLE
Business Process Understanding
Segregation & Controls
Key Performance Measurement
System Implementation
System Evaluation & Selection
System Audit & Review
Business Process Re-engineering
Policies, Procedures & Reporting
Roles & Responsibilities
PROCESS
TECHNOLOGY


Strategy
People
Technology
Process
Compliance
Project Management
Change Management


Continuous Improvement
People
Process
Technology

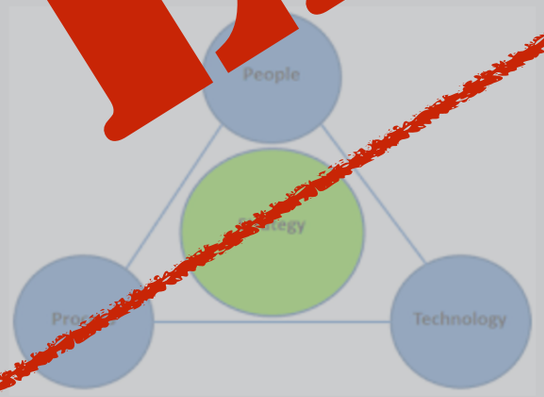

Process
Technology

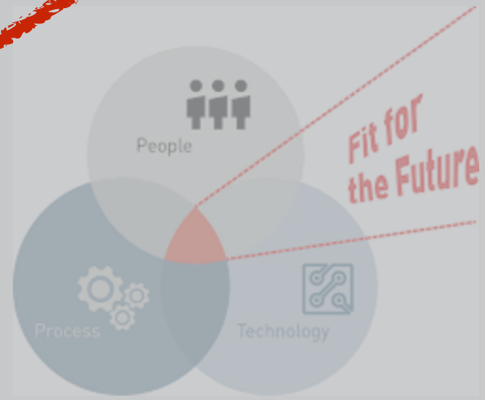

PROCESS
PEOPLE
SUCCESS
TECHNOLOGY

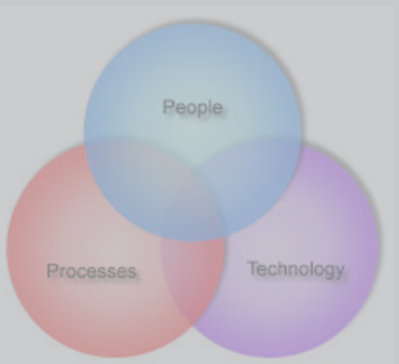

Process
Technology
People


People
Process
Technology


People
Process

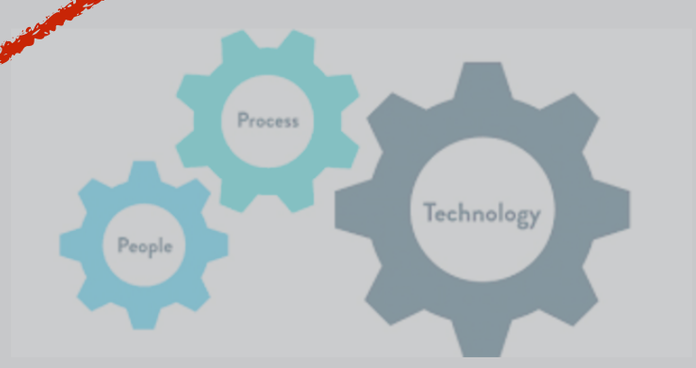

People
Technology


People
Process
Technology
Fit for the Future


People
Processes
Technology


Process
• Align tasks to milestones
• Re-define work flow
• Standardise library nomenclature
• Activate vendor Portal
• Create task dependencies

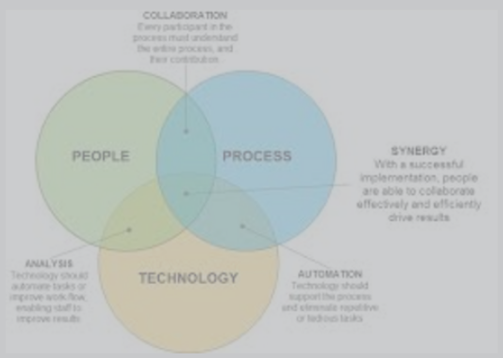

People, Process & Technology
Intelligence
Operations
Visibility
ISSA


Process
People
Technology


MONITORING
TROUBLE-SHOOTING
PEOPLE
TECHNOLOGY
PROCESS
IMPROVEMENT
REMEDIATION


firehost
People, Process, & Technology
PEOPLE
PROCESS
TECHNOLOGY


People
Process
Technology


COLLABORATION
PEOPLE
PROCESS
SYNERGY
With a successful implementation, people are able to collaborate effectively and efficiently drive results
TECHNOLOGY
ANALYSIS
AUTOMATION




PEOPLE
PROCESS
TECHNOLOGY

PEOPLE



Security Princess
@laparisa

Following

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 253 LIKES 237



4:01 AM - 25 Apr 2015

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

many org's will happily pay millions for shiny, blinky boxes

but will consider it outrageous to pay the same for quality people

if you are a manager, and recognise this about your org

fixing that will be a far better spend of your time, than chasing password change policies..

How many people do you need?



Andrew Case @attrc · Apr 9

@alexcpsec @rich0H when they have a sec team and org as big as google, MS, etc. then they can be trusted (to an extent) with such data.

https://twitter.com/attrc/status/718884779849052160



Andrew Case @attrc · Apr 9

@alexcpsec @rich0H when they have a sec team and org as big as google, MS, etc. then they can be trusted (to an extent) with such data.



ryan huber
@ryanhuber

Following

@attrc @alexcpsec @rich0H Couldn't agree more! I've always said headcount is the absolute best metric for judging a security team.

LIKES
6



12:13 AM - 10 Apr 2016

https://twitter.com/ryanhuber/status/718924951177138176

“Distributed Security Alerting”



Ryan Huber

Mar 1 · 5 min read

https://slack.engineering/distributed-security-alerting-c89414c992d6#.caybtgv3q







Several People Are Coding

3



Ryan Huber
Mar 1 · 5 min read

Recommended by Adrian Sanabria, M.G. Siegler, and 96 others

Distributed Security Alerting

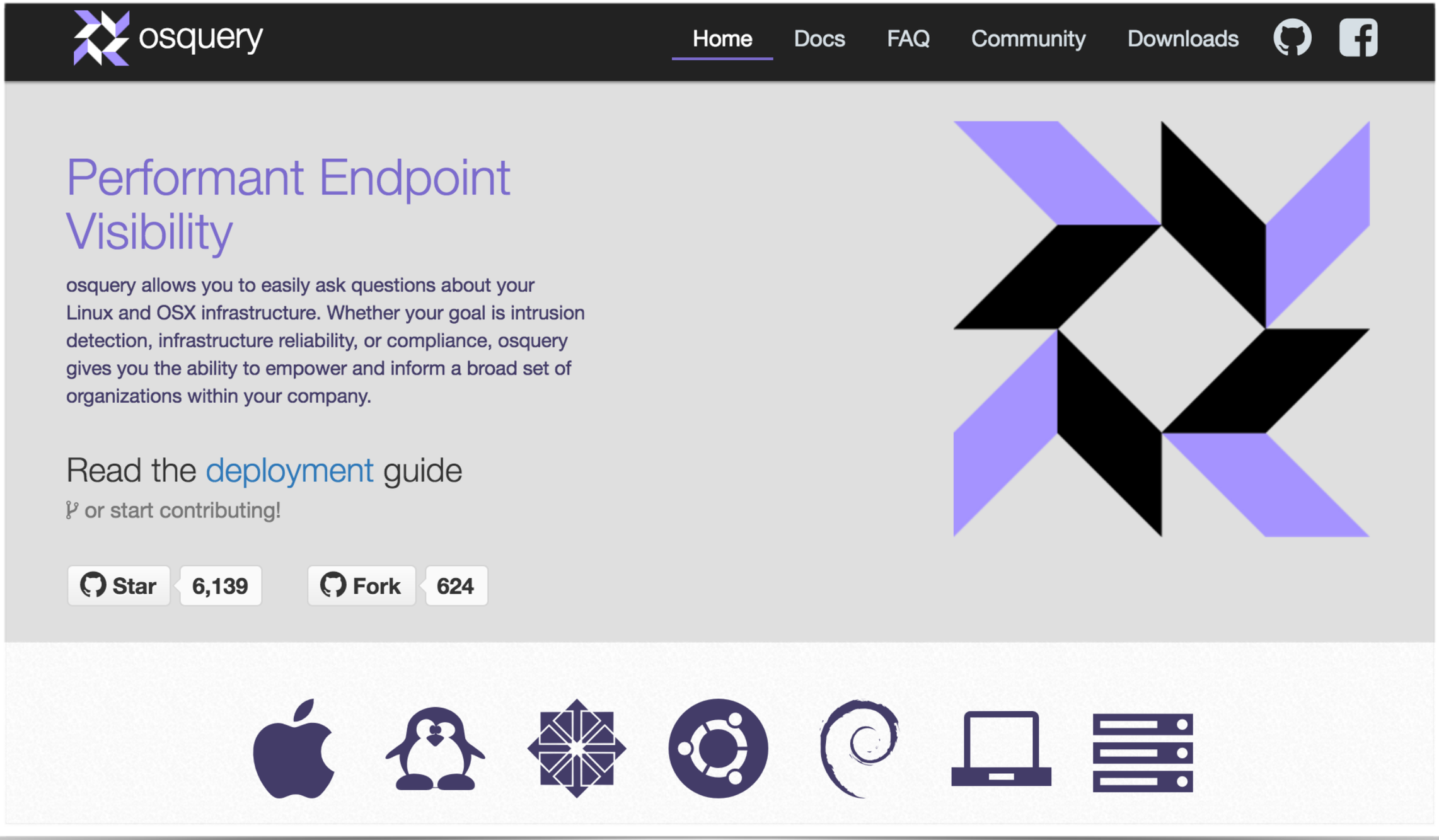


https://slack.engineering/distributed-security-alerting-c89414c992d6#.caybtgv3q

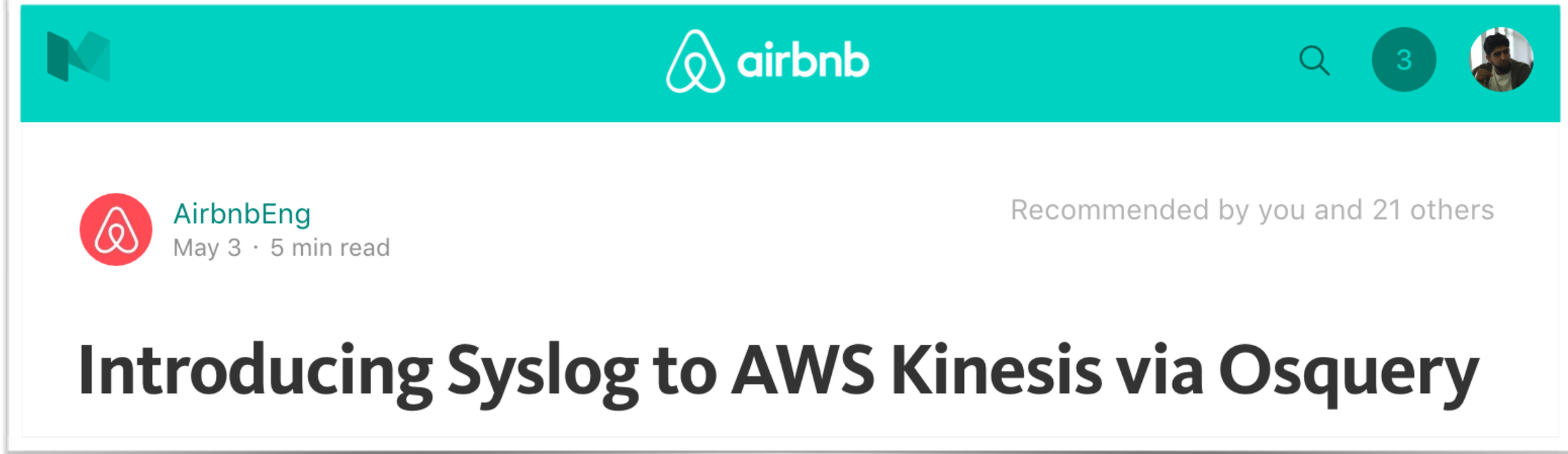
1) Why are we failing?

2) Is anyone succeeding?

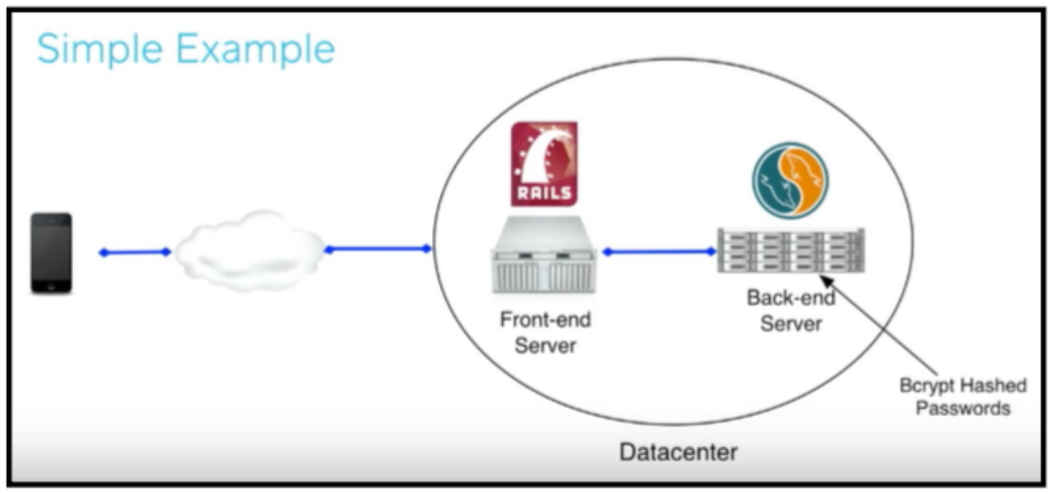
facebook, slack, etsy, square, airbnb..



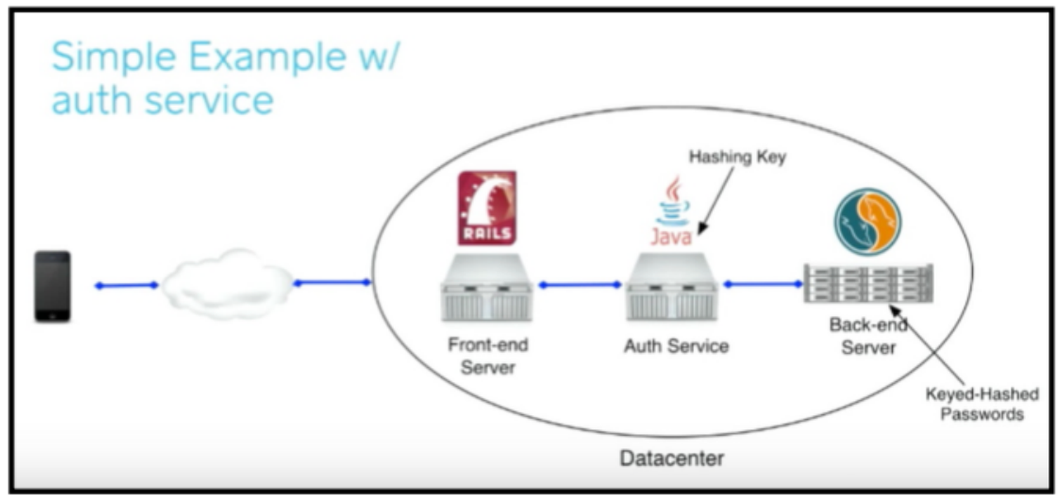
https://osquery.io/



https://medium.com/airbnb-engineering/introducing-syslog-to-aws-kinesis-via-osquery-da4fc19de5ce#.cfg8a4w3n



to





https://www.youtube.com/watch?v=lrGbK6fE7bI

facebook

2FAC: Facebook's internal multi-factor auth platform

Facebook Security

https://www.youtube.com/watch?v=pY4FBGI7bHM

http://research.google.com/pubs/pub43231.html

BeyondCorp

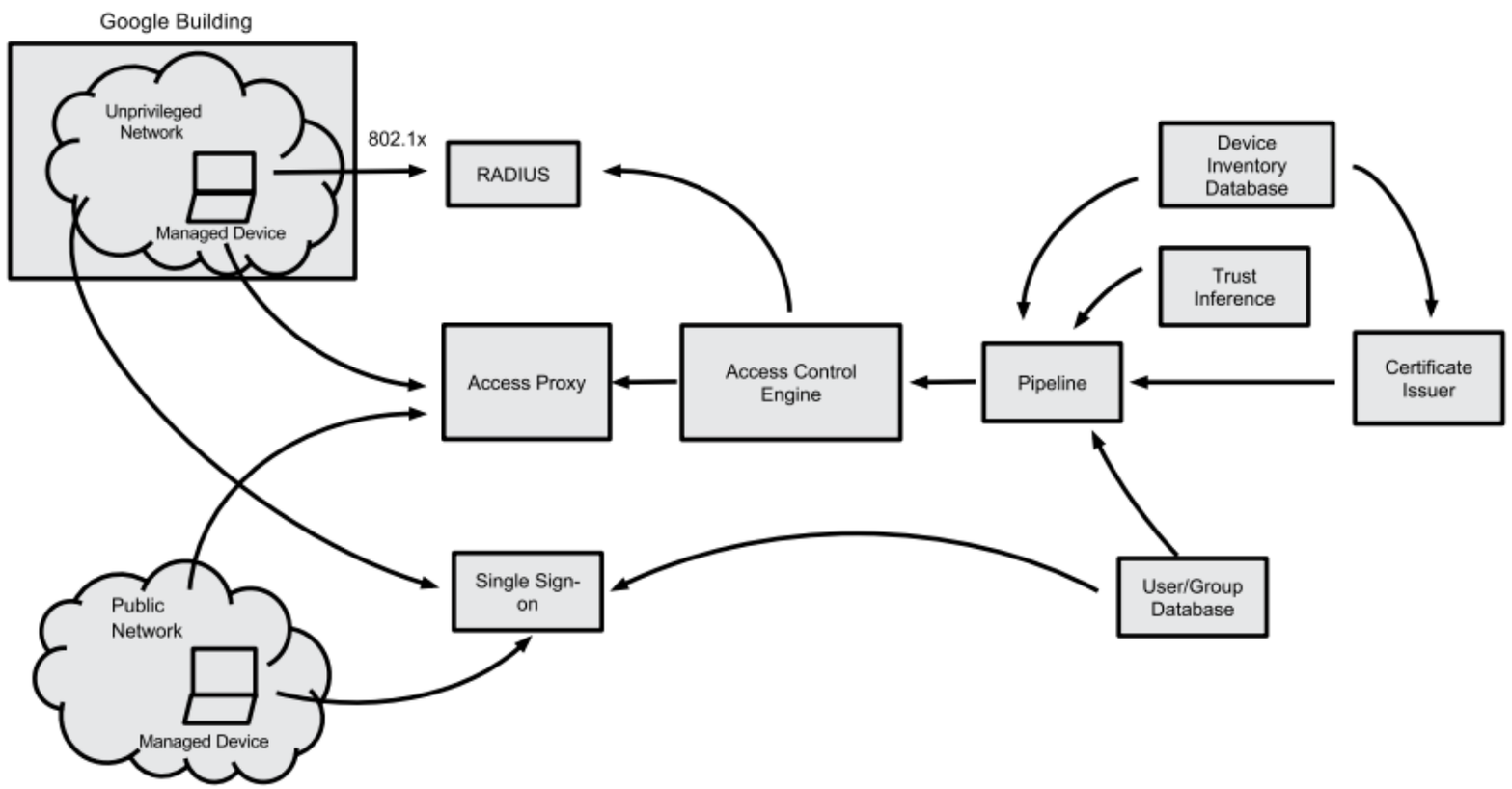
A New Approach to Enterprise Security

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

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



What do we notice?





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

Why Software Is Eating The World

By MARC ANDREESSEN

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoni
PC business in favor of investing more heavily in software, where it sees better potential for gr
Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised
But both moves are also in line with a trend I've observed, one that makes me optimistic about
of the American and world economies, despite the recent turmoil in the stock market.



In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc Andreessen insists that the recent popularity of tech companies does not constitute a bubble. He also stressed that both Apple and Google are undervalued and that "the market doesn't like tech."

In short, software is eating the world.

More than 10 years after the peak of the 1990s
a dozen or so new Internet companies like Fac
Twitter are sparking controversy in Silicon Va
rapidly growing private market valuations, an
occasional successful IPO. With scars from th
Webvan and Pets.com still fresh in the investo
are asking, "Isn't this just a dangerous new bu

I, along with others, have been arguing the otl
case. (I am co-founder and general partner of
firm Andreessen-Horowitz, which has investe

software is a force multiplier

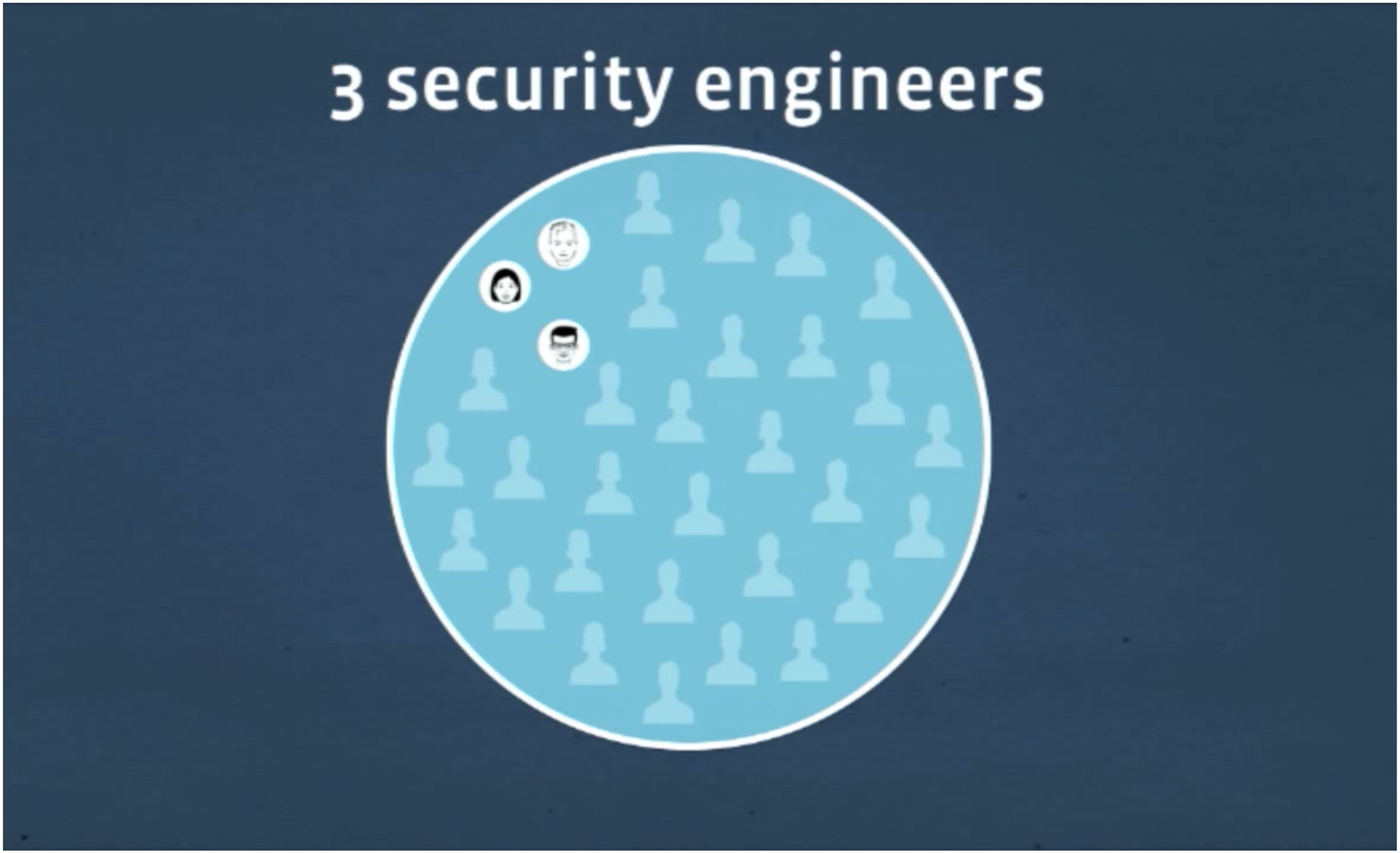
Mobile development @ Scale



100s of engineers

> 150K files

> 100K commits


3 security engineers

Security ppl that enable business

Enabling

A security team's success should be measured by what they enable not by what they block

Etsy

@iodboi

https://speakerdeck.com/iodboi/crafting-an-effective-security-organisation-qcon-nyc

https://speakerdeck.com/iodboi/crafting-an-effective-security-organisa

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://speakerdeck.com/iodboi/crafting-an-effective-security-organisation-qcon-nyc

Can we afford those guys?

Can we afford not to have them?

How do we get there?

Paul Graham

“The Design Paradox”

http://paulgraham.com/gh.html

Some heuristics

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

Etsy

@iodboi

https://speakerdeck.com/iodboi/crafting-an-effective-security-organisation-qcon-nyc

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://speakerdeck.com/iodboi/crafting-an-effective-security-organisation-qcon-nyc

Makes Realistic Tradeoffs

- Not everything is critical
- Understand impact
- Let low risk issues ship & getting commitments to a reasonable remediation window buys you lots
- **No's are a Finite Resource** - use them wisely

Etsy @iodboi

https://speakerdeck.com/iodboi/crafting-an-effective-security-organisation-qcon-nyc

People who (can) think like attackers

!=

People who can attack things

In Summary..

- Our old way clearly wasn’t working;
- Enterprise Sec is an engineering problem;
- We can’t outsource our thinking;
- Great things happen when you hire good people.



Questions?

http://thinkst.com | @haroonmeer