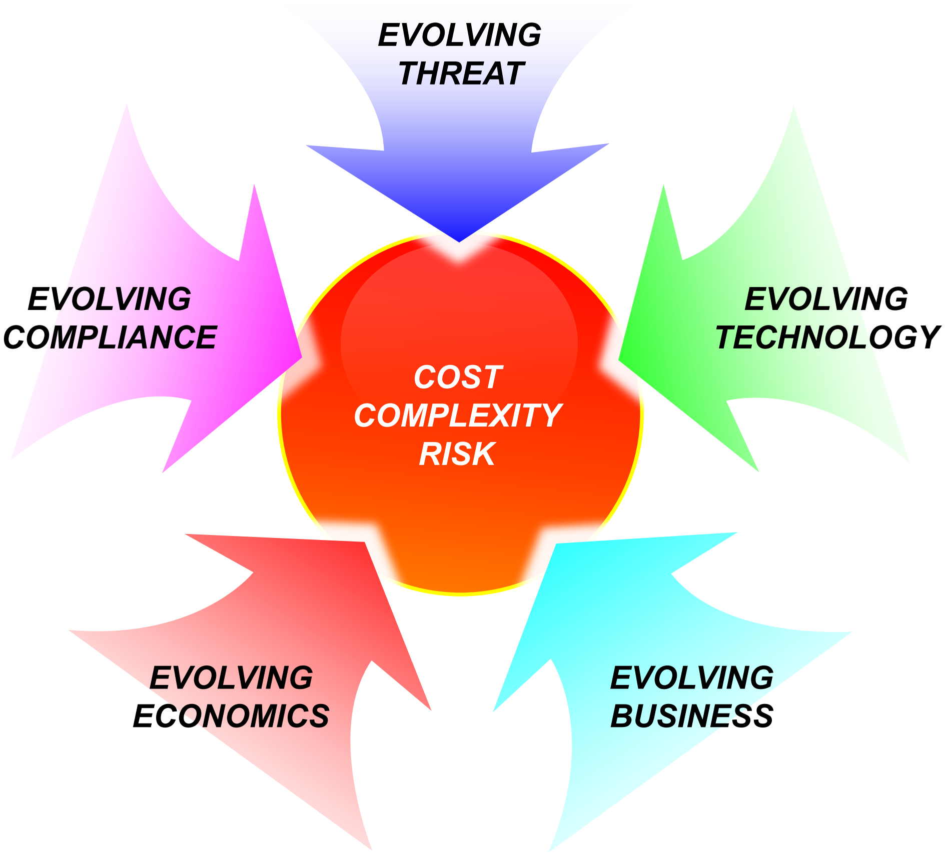
Rugged Software Development

Joshua Corman, David Rice, Jeff Williams

SANS Application Security Summit

February 5, 2010

Context


EVOLVING THREAT
EVOLVING COMPLIANCE
EVOLVING TECHNOLOGY
COST
COMPLEXITY
RISK
EVOLVING ECONOMICS
EVOLVING BUSINESS

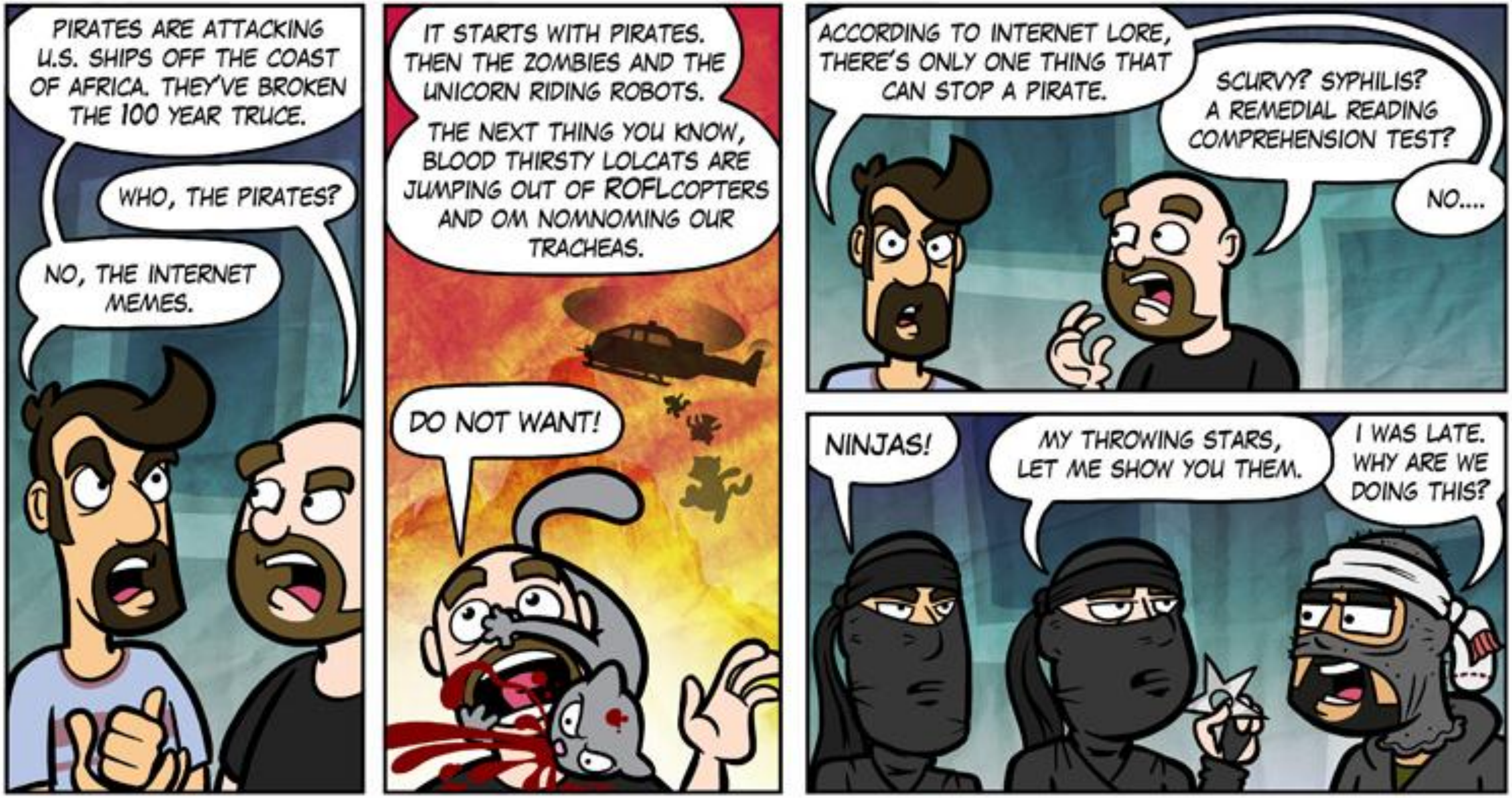
GREYLOCK PARTNERS

“What is missing from software security?”

CULTURAL INFORMATION
PRACTICE OR IDEA OR CONCEPT
THEORIES PRACTICES HABITS SONGS
NATURAL SELECTION
EXAMPLES MIGHT INCLUDE THOUGHTS IDEAS
CHARLES DARWIN'S IDEAS
SELF-PROPAGATING
SURVIVAL AND COMPETITION INFLUENCE THEM

MEME

DANGER
MEMES
AHEAD

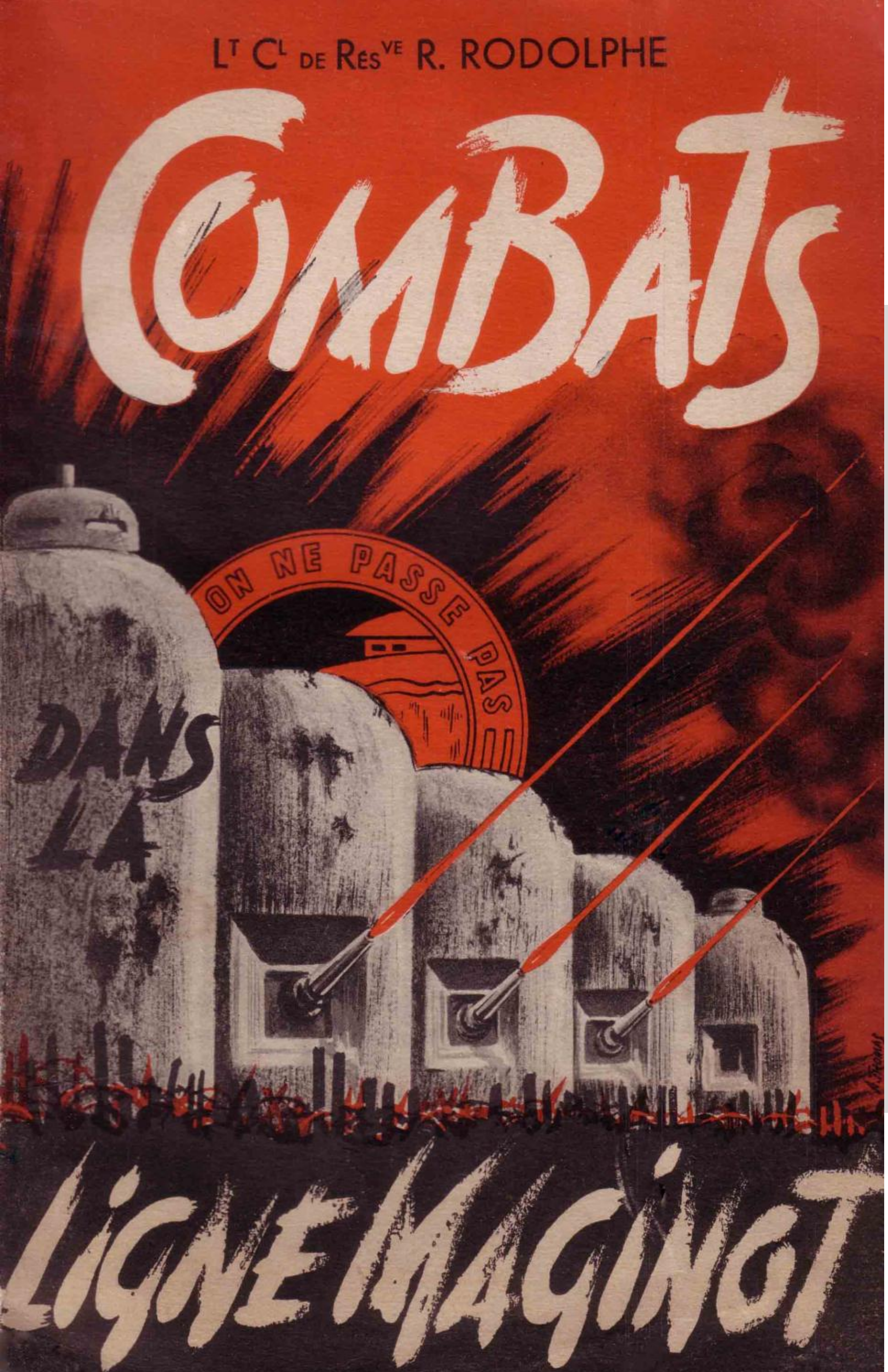

PIRATES ARE ATTACKING U.S. SHIPS OFF THE COAST OF AFRICA. THEY'VE BROKEN THE 100 YEAR TRUCE.
WHO, THE PIRATES?
NO, THE INTERNET MEMES.
IT STARTS WITH PIRATES. THEN THE ZOMBIES AND THE UNICORN RIDING ROBOTS.
THE NEXT THING YOU KNOW, BLOOD THIRSTY LOLCATS ARE JUMPING OUT OF ROFLCOPTERS AND OM NOMNOMING OUR TRACHEAS.
DO NOT WANT!
ACCORDING TO INTERNET LORE, THERE'S ONLY ONE THING THAT CAN STOP A PIRATE.
SCURVY? SYPHILIS? A REMEDIAL READING COMPREHENSION TEST?
NO....
NINJAS!
MY THROWING STARS, LET ME SHOW YOU THEM.
I WAS LATE. WHY ARE WE DOING THIS?

© 2009 JOEL WATSON WWW.HIJINKSENSUE.COM

Google
CHINA
THERE IS NOTHING MORE ANNOYING ON THE WEB THAN AN UNWANTED Pop-up!

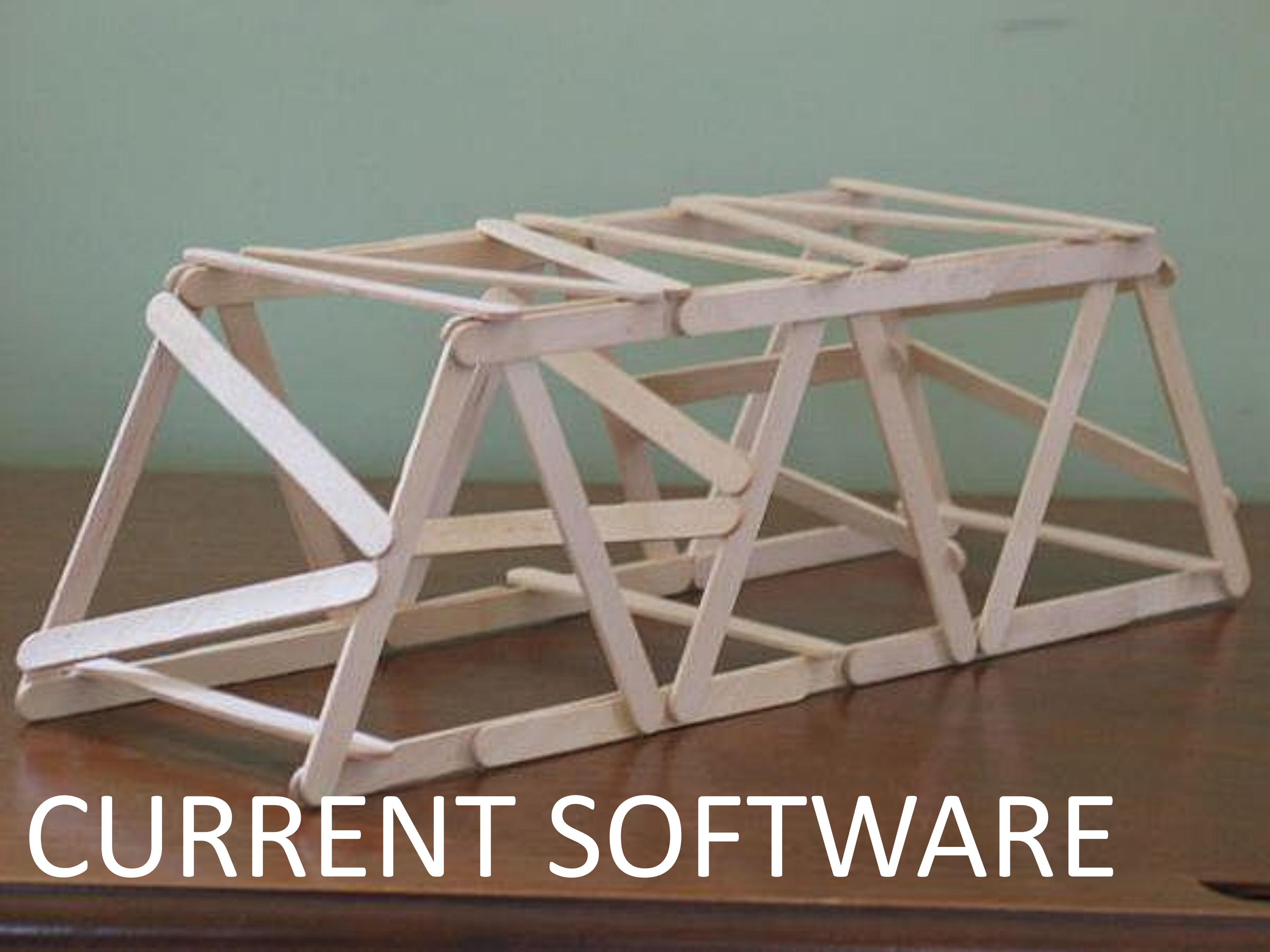
Secure software is critically important to almost every aspect of life.

© The Economist, January 16, 2010



“A fortress mentality will not work in cyber. **We cannot retreat behind a Maginot Line of firewalls**…If we stand still for a minute, our adversaries will overtake us.”

-William Lynn, U.S. Deputy Secretary of Defense
January 2010



CURRENT SOFTWARE

RUGGED SOFTWARE

CURRENT SOFTWARE

RUGGED SOFTWARE

CURRENT SOFTWARE

RUGGED SOFTWARE

…so software not only needs to be…

projectiondesign
Coca-Cola
1
Radisson SAS
PLAZA HOTEL OSLO
SIEMENS
hydrolift
fly without wings
Koenigsegg
Steve Curtis
spirit of NORWAY
OFFSHORE RACING
Color Line
spiritofnorway.com

FAST

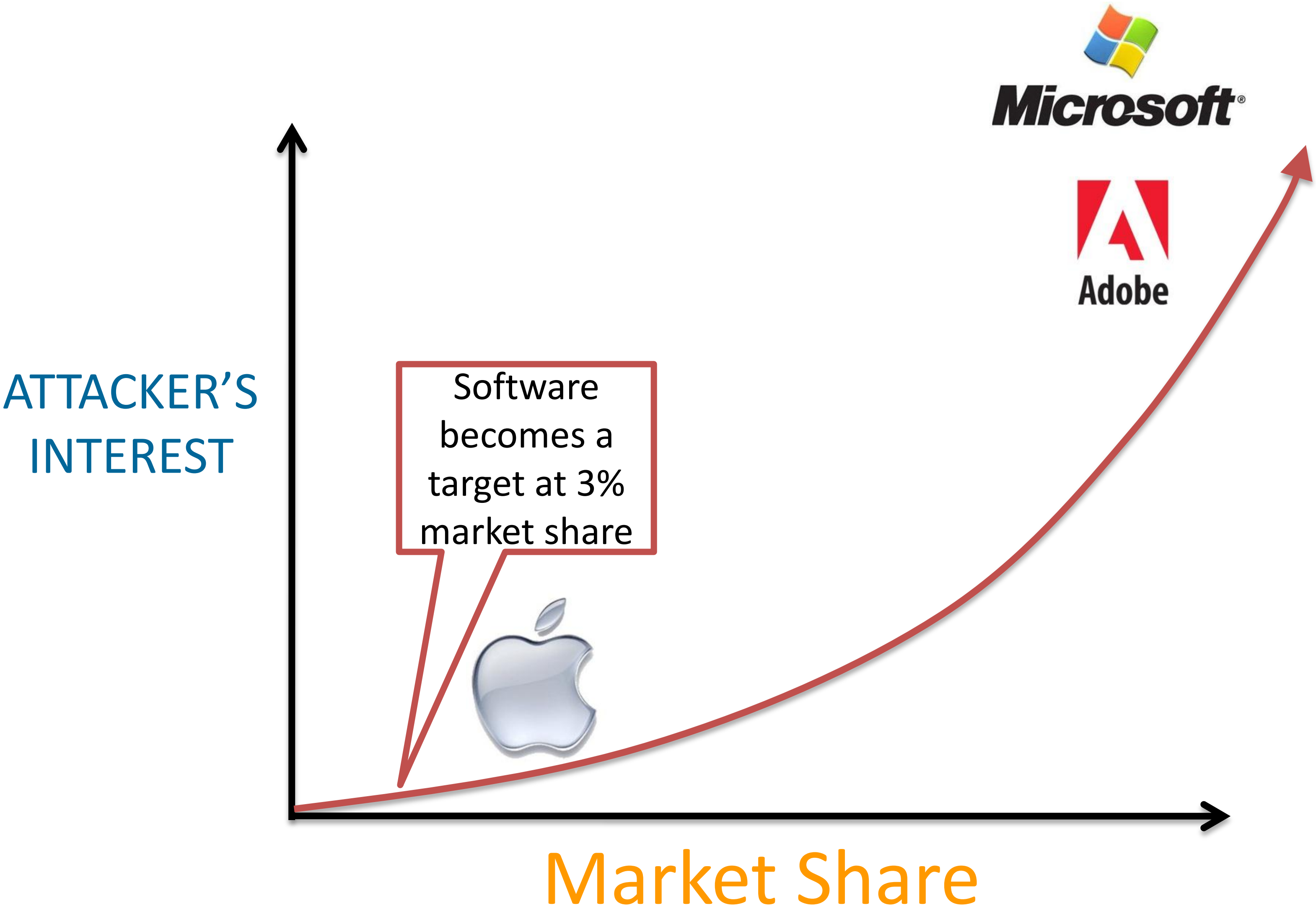
AGILE

Are You Rugged?

HARSH

UNFRIENDLY

There is no such thing as “toy” software.



ATTACKER'S INTEREST

Software becomes a target at 3% market share

Market Share

THE MANIFESTO

I am rugged - and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

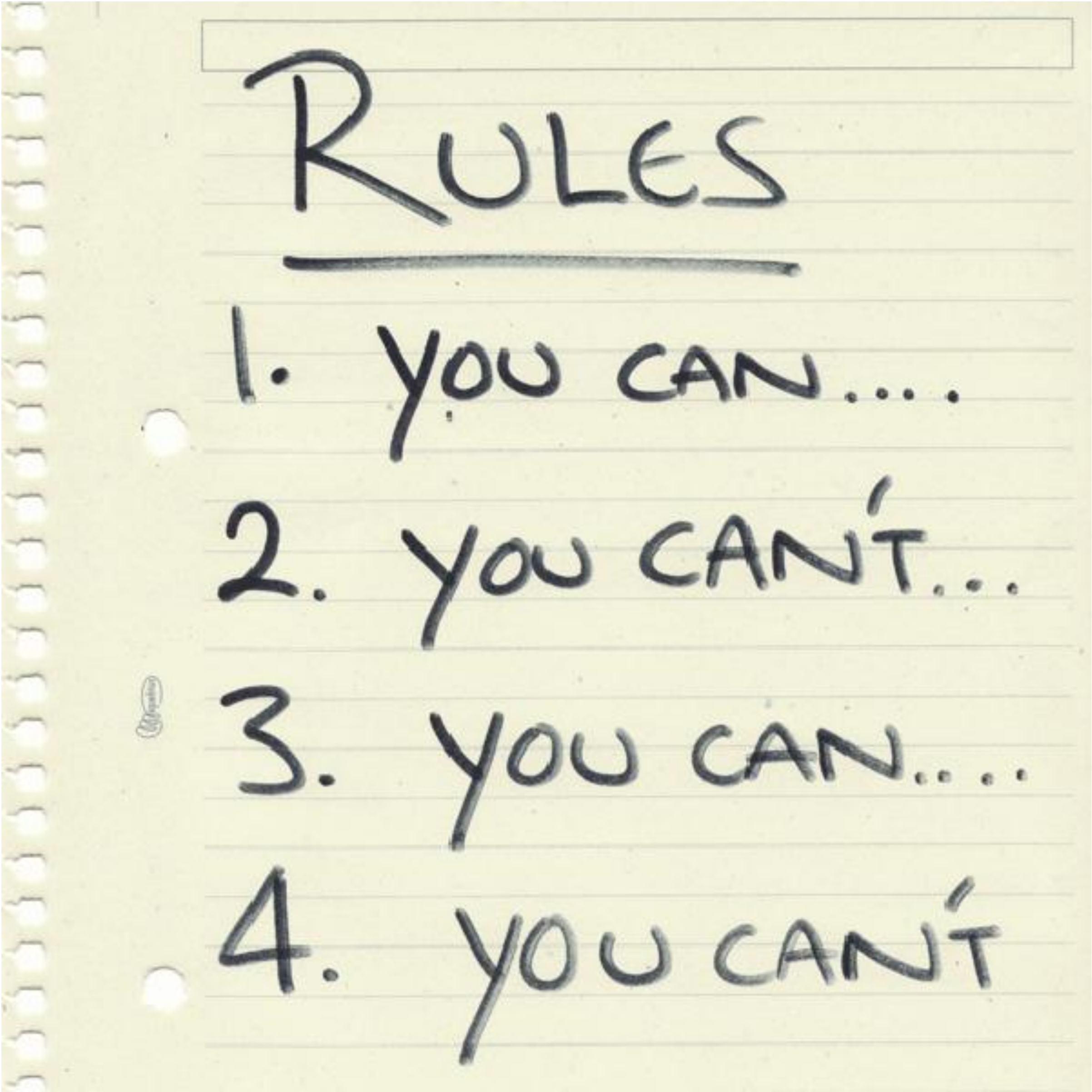
I am rugged, not because it is easy, but because it is necessary… and I am up for the challenge.

Rugged?

WHAT IS RUGGED?

It’s not about style, it’s about the result.

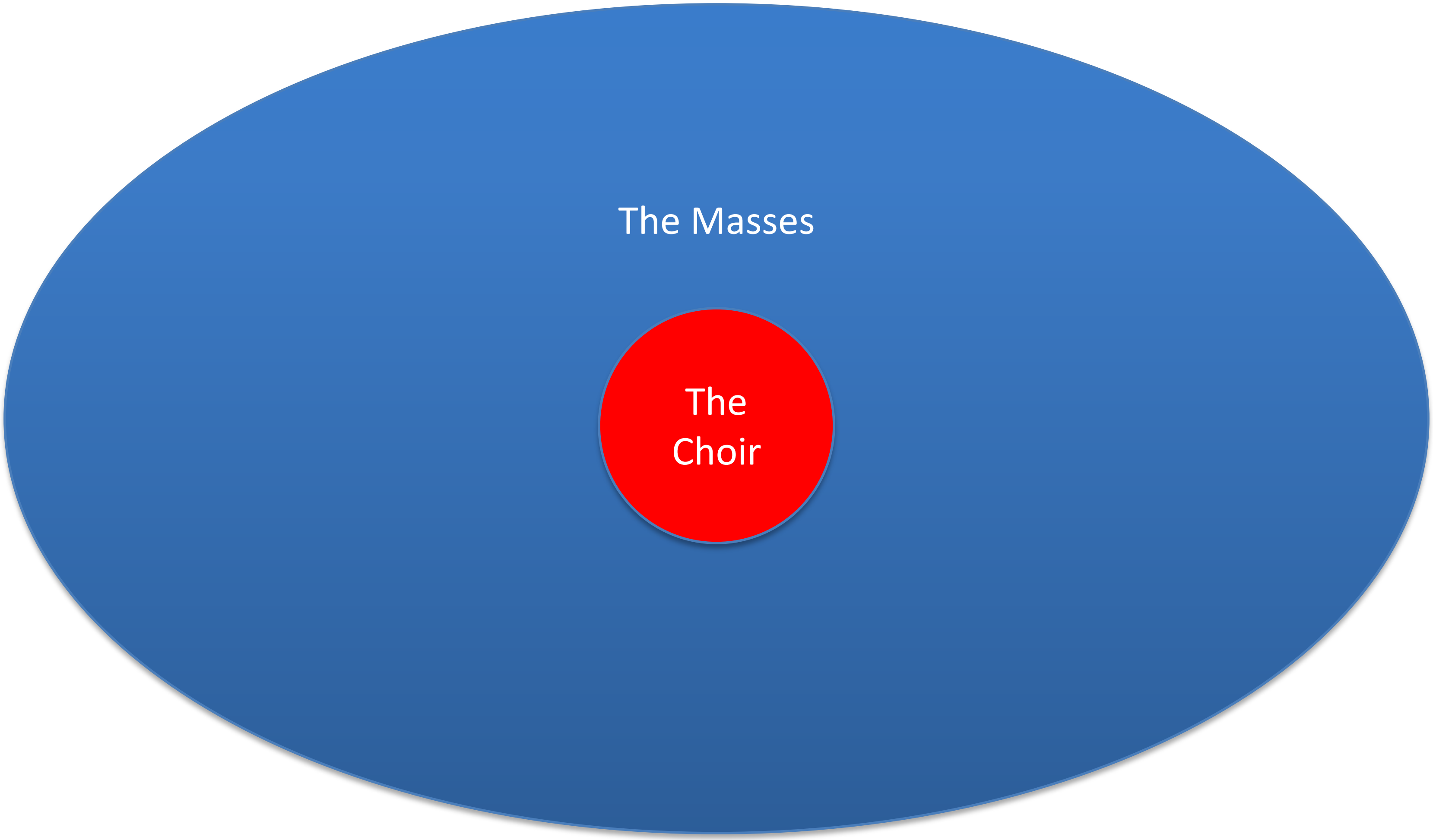
It’s not about external compliance…



RULES

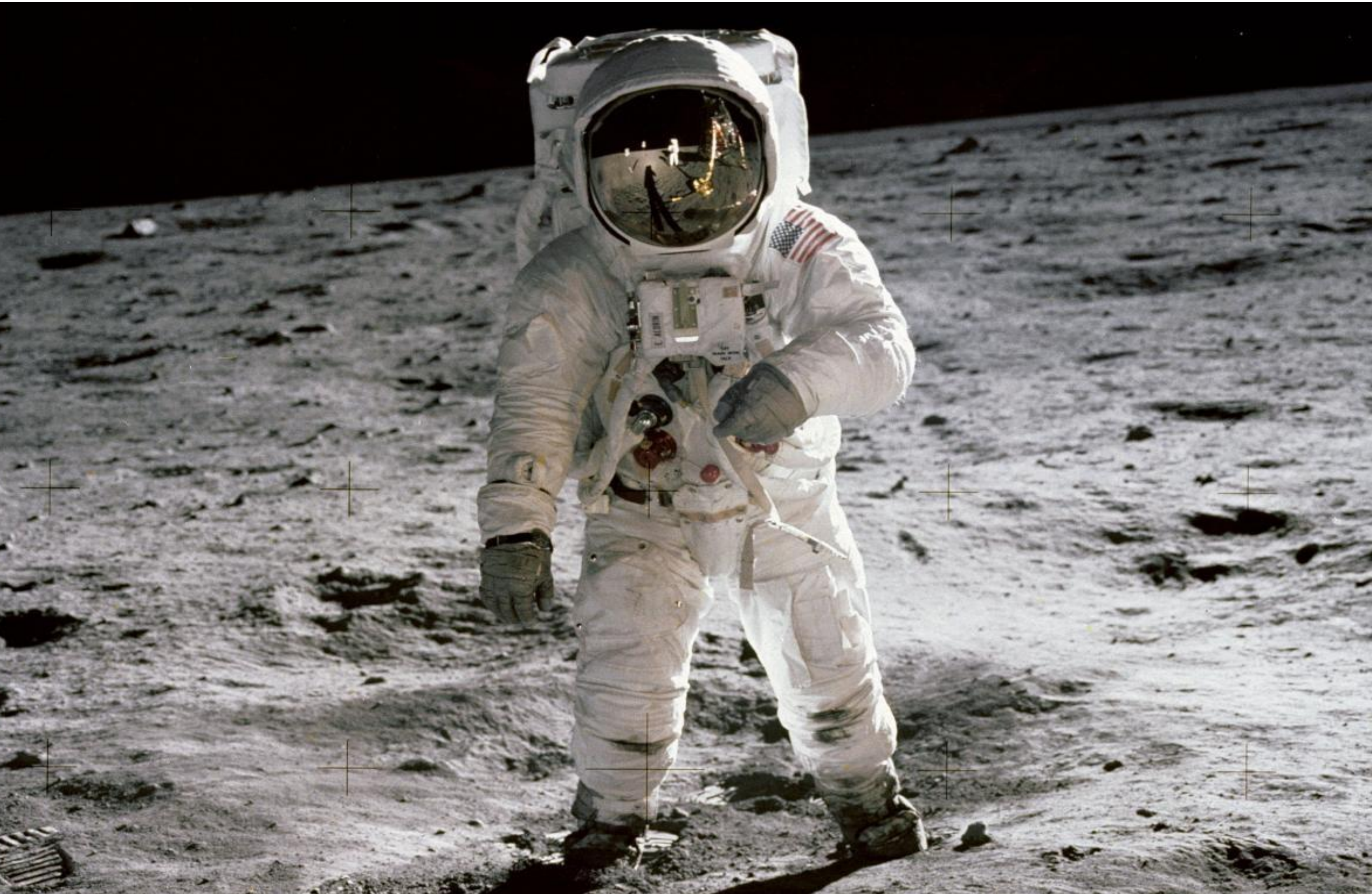
1. YOU CAN....
2. YOU CAN'T...
3. YOU CAN....
4. YOU CAN'T

1) Beyond the choir

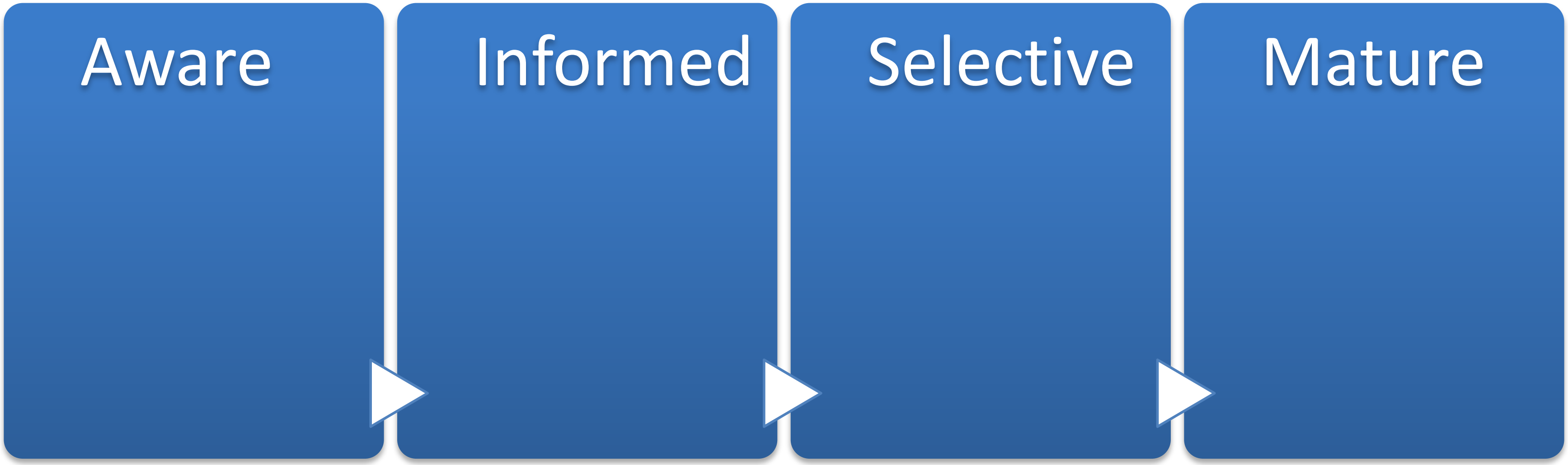


2) Beyond technology

3) Aspirational



The Journey



Aware

Informed

Selective

Mature

GETTING INVOLVED

Folks Who Helped Shape This

- Dan Geer, In-Q-Tel
- Chris Hoff, Cisco
- Chris Wysopal, Veracode
- Scott Crawford, EMA
- Pete Lindstrom, Spire Security
- Andrew Hay
- Tom Kellermann, Core Security
- Will Gragido, Cassandra Security
- Eric Hanselman, LeoStream
- Marisa Fagan, Errata Security
- Anton Chuvakin, Security Warrior
- Joe Jarzombek, DHS
- Barmak Meftah, Fortify
- Nick Selby, Trident Risk Mngt
- David Etue, Fidelis
- Rich Mogull, Securosis
- Adrian Lane, Securosis
- Tim Greene, NetworkWorld
- Dan Guido, NYU: Poly
- Caleb Sima, HP
- Ryan Barnett, Breach Security
- Jack Daniel, Astaro
- Jennifer Jabbusch, CAD, Inc.

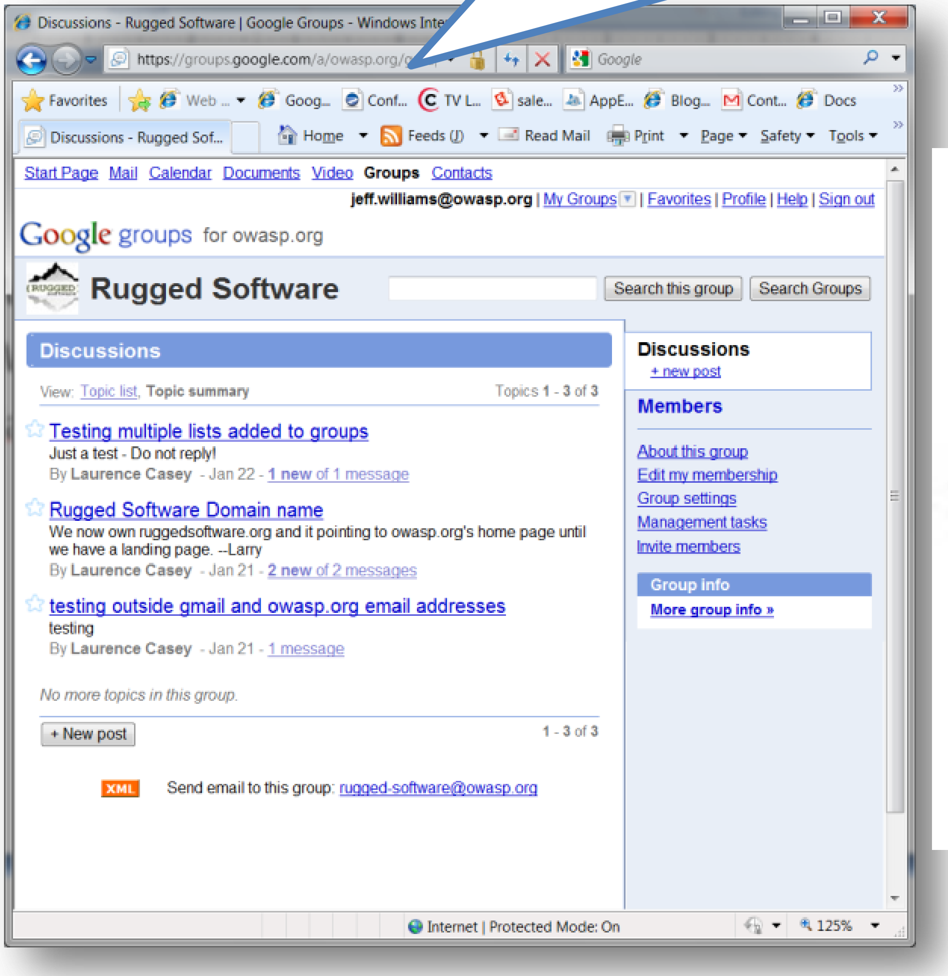
Next Steps…

- Charter Members
- Introductions to University CS Programs
- Chair and Co-Chair Working Groups
  - Welcome Package: Getting Started
  - Business Cases

How to find out more…

http://ruggedsoftware.org

https://groups.google.com/a/owasp.org/group/rugged-software


Discussions - Rugged Software | Google Groups - Windows Inte
https://groups.google.com/a/owasp.org/g
Google
Favorites
Web ...
Goog...
Conf...
TV L...
sale...
AppE...
Blog...
Cont...
Docs
Discussions - Rugged Sof...
Home
Feeds (J)
Read Mail
Print
Page
Safety
Tools
Internet | Protected Mode: On
125%

Start Page Mail Calendar Documents Video **Groups** Contacts

jeff.williams@owasp.org | My Groups | Favorites | Profile | Help | Sign out

Google groups for owasp.org

Rugged Software

Search this group | Search Groups

Discussions

View: Topic list, **Topic summary** Topics **1 - 3** of **3**

Testing multiple lists added to groups
Just a test - Do not reply!
By **Laurence Casey** - Jan 22 - **1 new** of 1 message

Rugged Software Domain name
We now own ruggedsoftware.org and it pointing to owasp.org's home page until we have a landing page. --Larry
By **Laurence Casey** - Jan 21 - **2 new** of 2 messages

testing outside gmail and owasp.org email addresses
testing
By **Laurence Casey** - Jan 21 - 1 message

No more topics in this group.

+ New post **1 - 3** of **3**

XML Send email to this group: rugged-software@owasp.org

Discussions
+ new post

Members

About this group
Edit my membership
Group settings
Management tasks
Invite members

Group info
More group info »

Google Groups

“What does Rugged mean to you?”