Responsibility for the Harm and Risk of Security Flaws

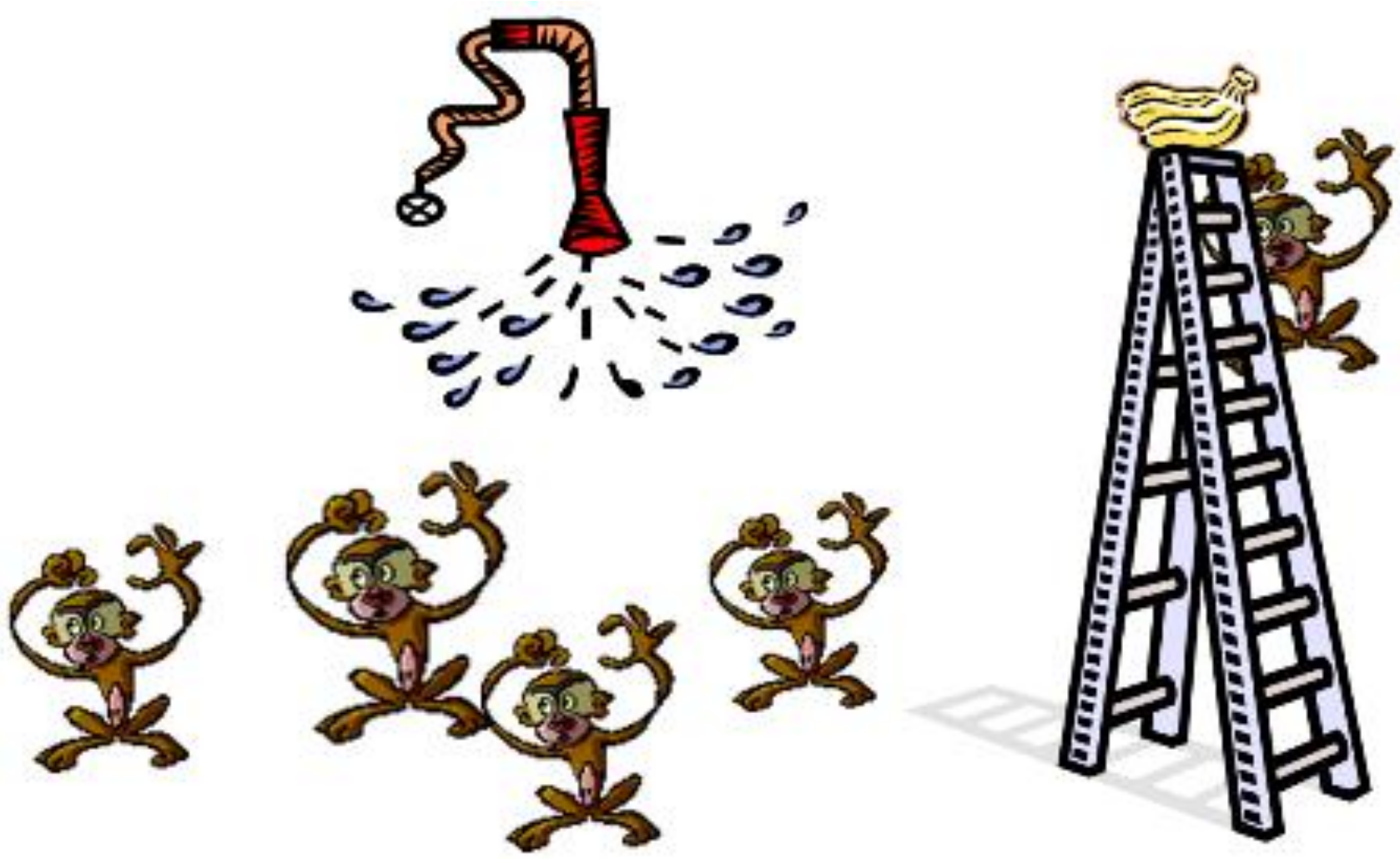
Cassio Goldschmidt

Sr. Manager, Product Security

What is Software?

Does it Matter?!?!

The Importance of Reviewing Our Beliefs



A Product

A Service

Speech

A Common Good

Common Goods can be “bad”

…and we all contribute to it.

…and we all contribute to it.
Today's Agenda

Corp. Users

Security Flaws

Manufacturers

Home Users

Sec. Researchers

Government

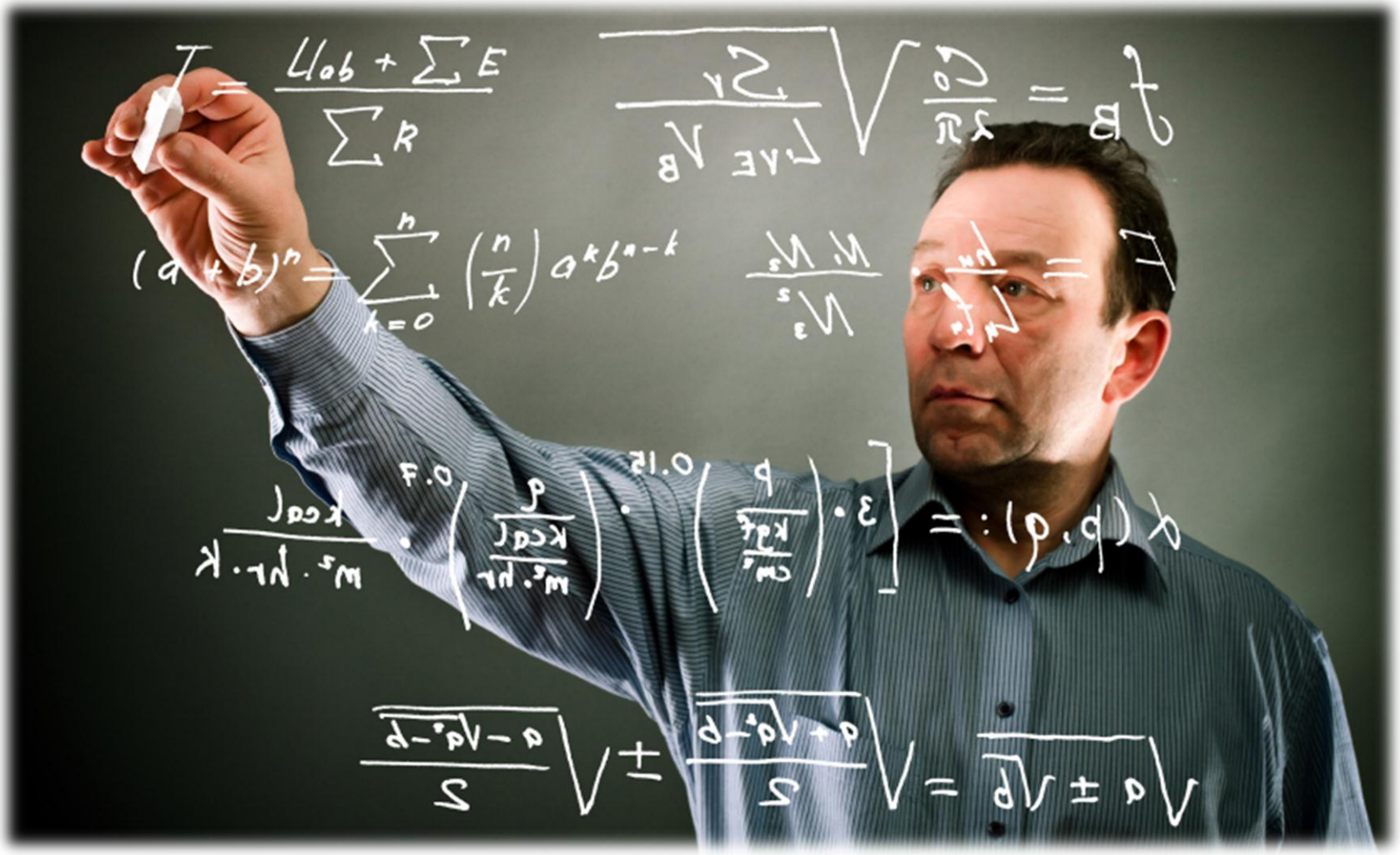
Manufacturers

Industry Best Practices – SAFECode.org

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

=

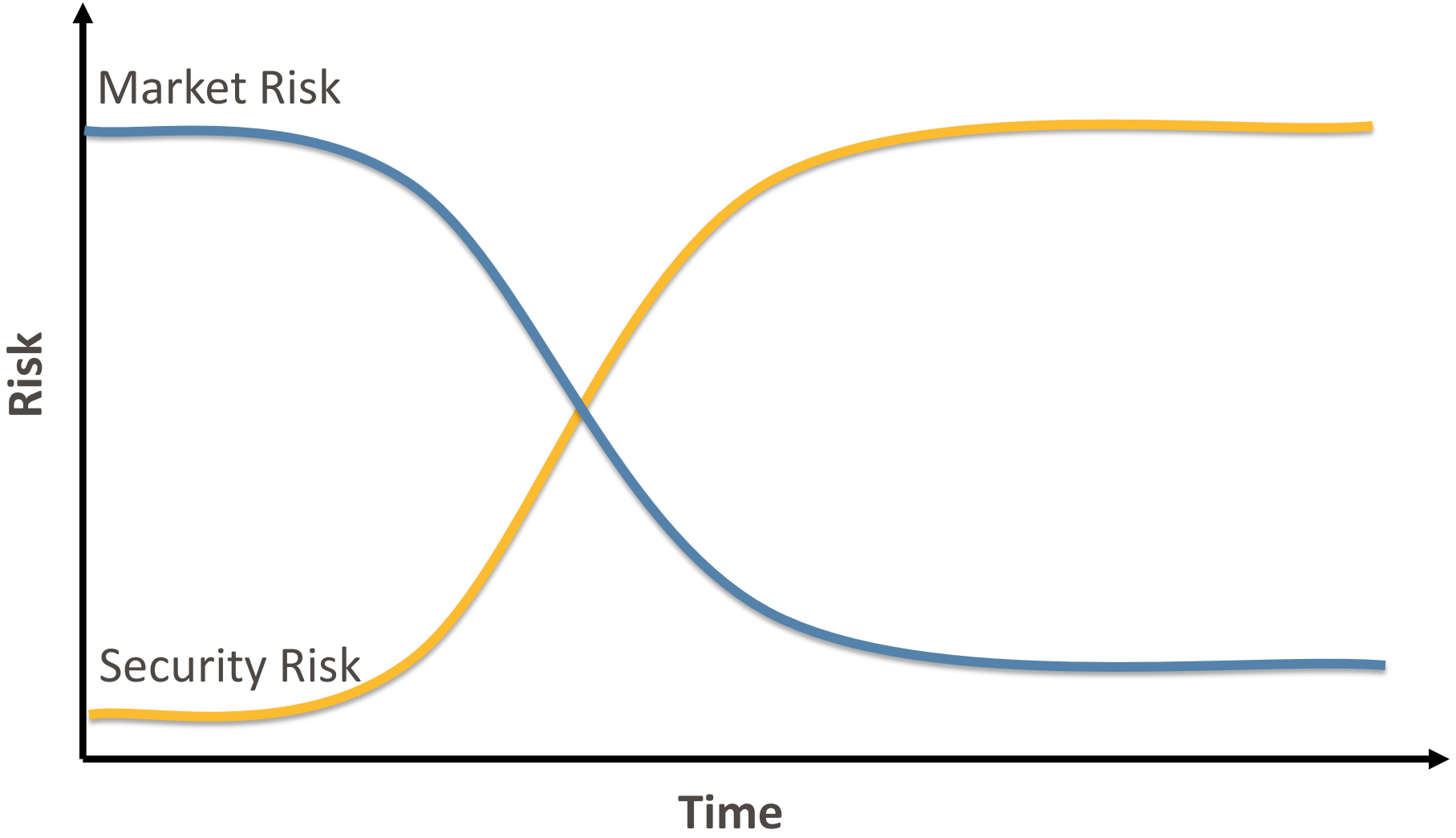
No Effective Way to Prove Software Correctness



The Weak Link

Investing in Security

The Business Definition of Risk



Adopters
(Home Users, Corporate Users)

Users Want Features

US$28,724

- Reliable

US$28,724

- Convertible
- Rear Spoiler
- Alloy Wheels
- And Red!

Security Is Not “Visible”

Will home users be able to tell which one is more secure?

US$99,999

US$28,724

Security Facts

Type: Web Application — Jun 28, 2010

OWASP Top 10 2010

A1-Injection	○
A2-Cross Site Scripting (XSS)	◒
A3-Authentication	●
A4-Object References	○
A5-Cross Site Request Forgery	○
A6-Security Configuration	○
A7-Cryptographic Storage	●
A8-URL Access Control	○
A9-Transport Layer Protection	◒
A10-Redirects and Forwards	○

Custom Code

Name	Languge	LOC
Core	Java	1200K
Developer Plugin	Java	20K
Reporting Plugin	Java	12K
Persistence Layer	PSQL	15K
User Interface	JSF	46K
Business Functions	Java	102K

Libraries

Name	Languge	H	U
Struts 1.1	Java	○	●
Log4j 1.0.3	Java	○	○
XOM 2.1	Java	◒	●
Hibernate 3.0	Java	●	○
OWASP ESAPI 2.0rc6	Java	●	●

Platform Components

Name	Languge	H	U
WebSphere 6.1.2	C/C++	●	●
Java Enterprise Edition 3.1	Java	●	○

Interfaces and Connections

Name	Protocol	D	E	N	Z
Web Interface	HTTPS	+	○	○	○
FTP Interface	FTP	+	●	●	●
Google Search API	REST	→	○	○	○
Sybase	TDS	↔	●	●	●
Oracle 11	SOAP	→	●	●	●
Log Server	SNMP	→	●	●	●
Mainframe	SNA	→	●	●	●

Sensitive Data

Name	Concerns	S	T	Z
Healthcare Records	CIA	●	◒	●
Credit Card Numbers	CI	●	○	◒

Application Security Program

Practice	Provider	M
Strategy and Metrics	Internal	○
Policy and Compliance	Internal	◒
Education and Guidance	Aspect Security	●
Threat Assessment	Internal	●
Security Requirements	Internal	●
Secure Architecture	Aspect Security	●
Design Analysis	Internal	○
Code Review	Aspect Security	●
Security Testing	Aspect Security	●
Vulnerability Mgmt	Internal	◒
Environment Hardening	Internal	○
Operational Enablement	Internal	●

Security Contact: security@aspectsecurity.com

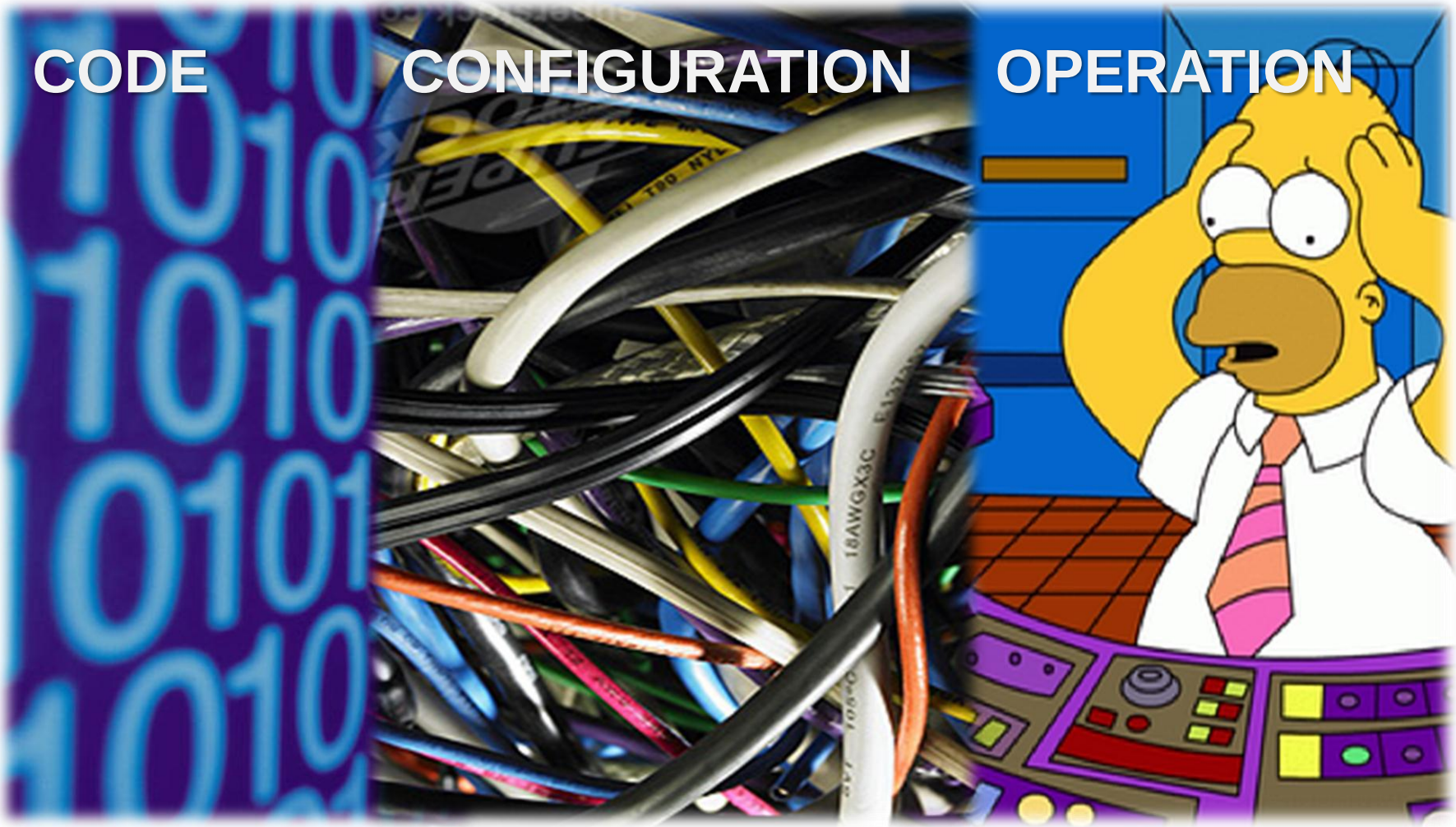
Network Effect Affects Decisions
Creation of an Ecosystem Affects Security

Ignoring updates put all of us at risk

- How often home users ignore this pop up?

Choosing to Adopt Software in Corporate Environments

Weakness Can Originate from Different Sources



Weakness Can Originate from Different Sources

Quarterly Freezes

December 2010

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1	2	3	4	5	6	7
8	9 	10 	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25 	26 	27	28
29 	30 	31 				

Security Researchers

Security Researchers

Full Disclosure

- All technical details are revealed.

Coordinated Disclosure

- Finders and manufacturers work together toward a solution.
- Coordinated Disclosure is the new Responsible Disclosure

Zero Day

- Technical details are published before the manufacturer is notified.

Security Researchers
Incentives and the Vulnerability Market

Sec. Researchers

Reward

Developer

Crime

Security Researcher Incentives and the Vulnerability Market

What happens when information leaks?

Government

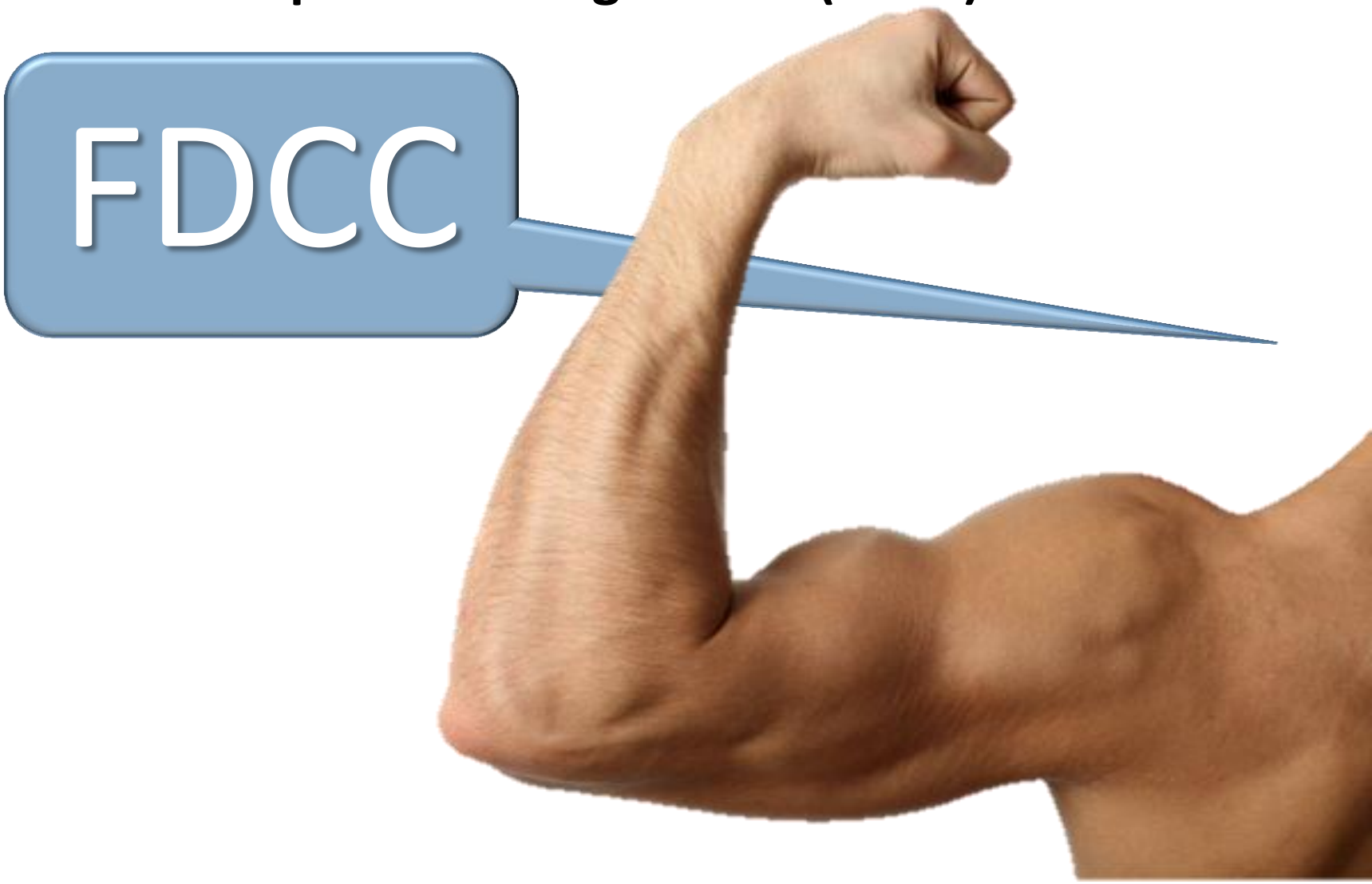
Government
Hacking Tools and Gun Laws

Government
Cutting Internet Access

Government Certifications

Government
Treating Vulnerabilities like Pollution

Government – Flexing its Muscles
Federal Desktop Core Configuration (FDCC)



Government
Too Early to Enact Laws?

Thank you!

This presentation is based on chapter 6 of "**Information Assurance & Security Ethics**" by Cassio Goldschmidt, Melissa Dark and Hina Chaudhry

ISBN: 978-1-61692-245-0 (hardcover)
ISBN: 978-1-61692-246-7 (ebook)

YouTube: www.youtube.com/cgoldsch