Responsibility for the Harm and Risk of Security Flaws
(Why Things are the Way They are)

Presented at OWASP AppSec Research 2010

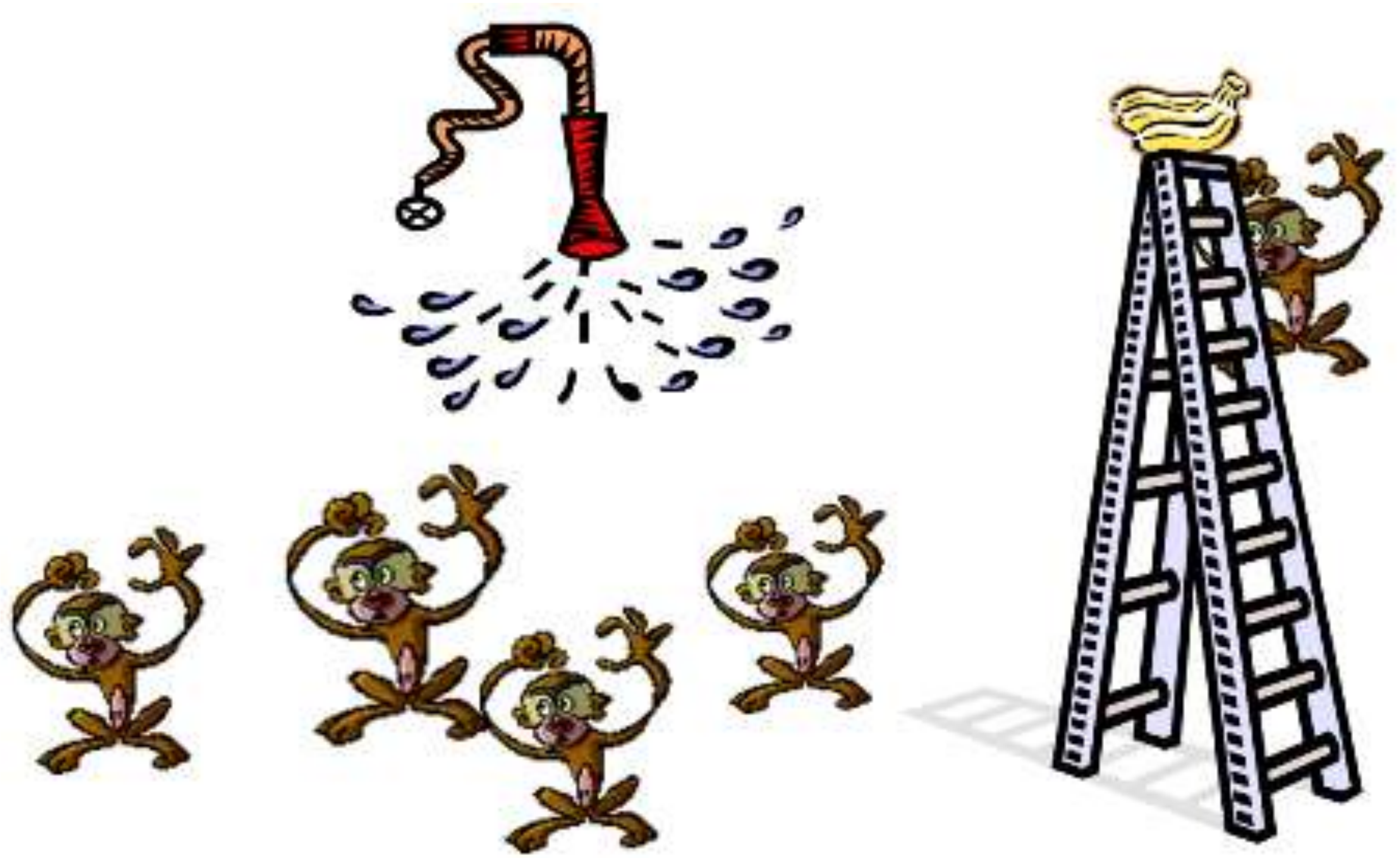
by Cassio Goldschmidt

Sr. Manager, Product Security

What is Software?

Does it Matter?!?!

The Importance of Reviewing Our Beliefs



A Product

A Service

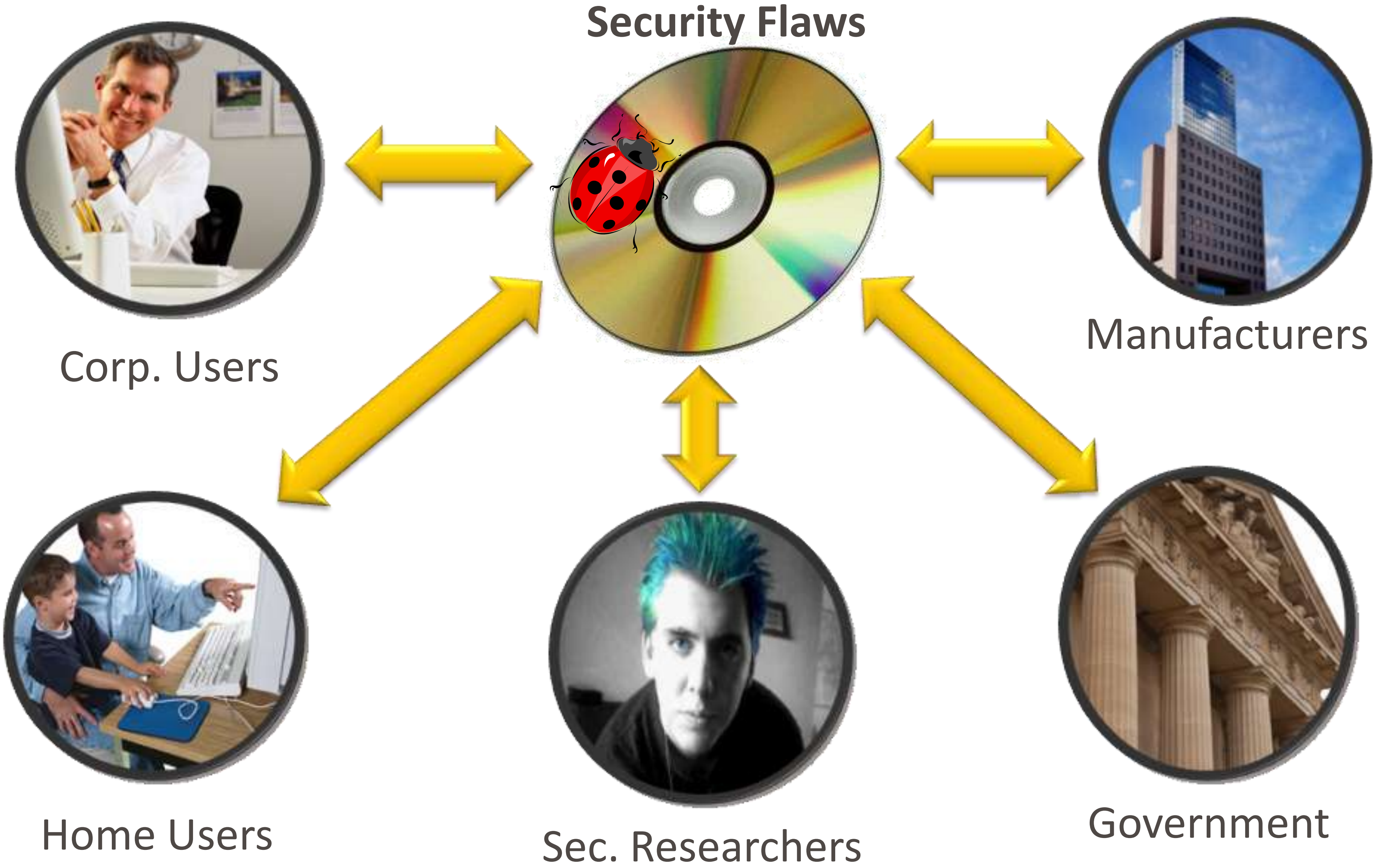
Speech

A Common Good

Common Goods can be "bad"

…and we all contribute to it.

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



Security Flaws

Corp. Users

Manufacturers

Home Users

Sec. Researchers

Government

Manufacturers

Industry Best Practices – SAFECode.org

SAFECode

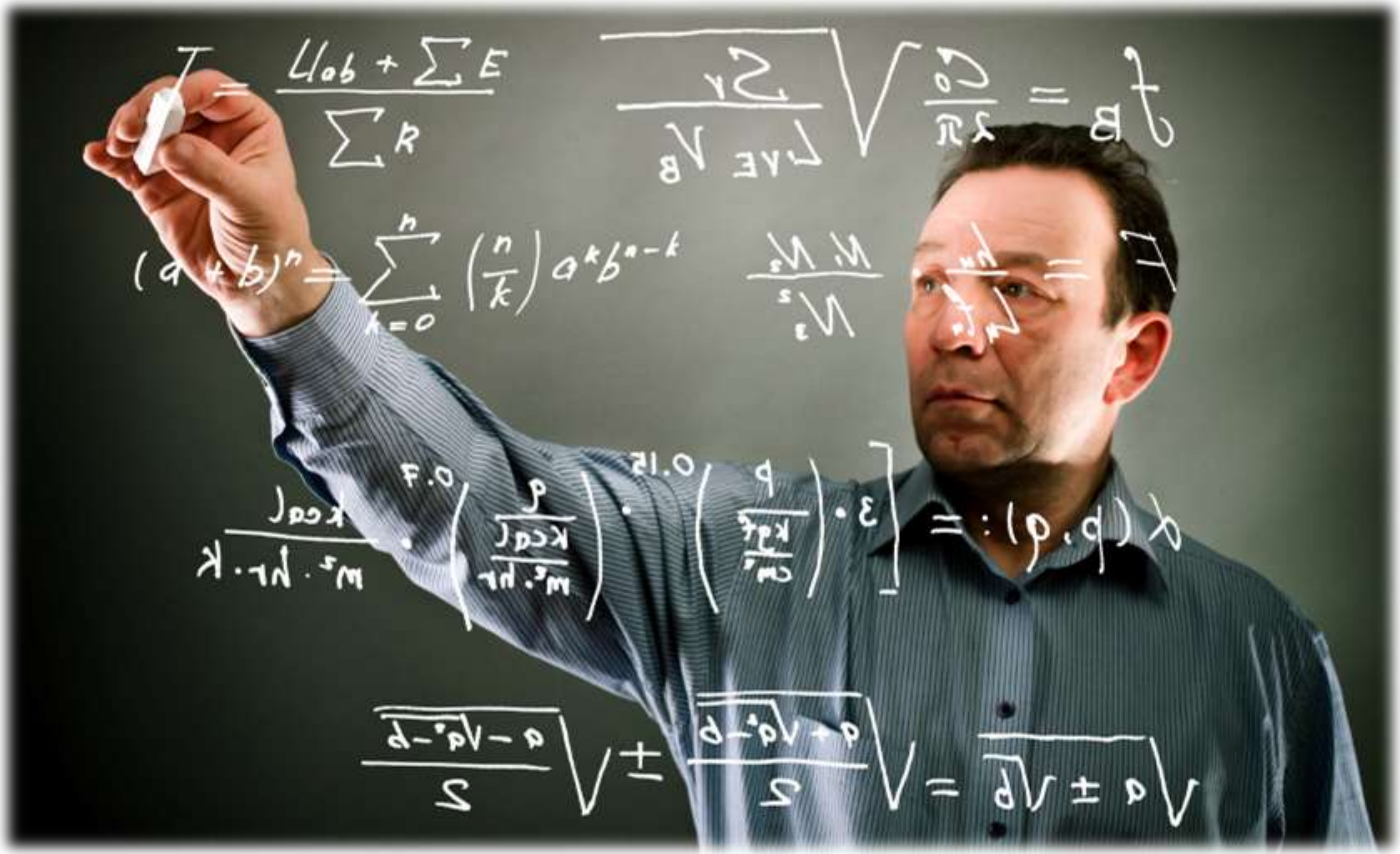
Software Assurance Forum for Excellence in Code

Driving Security and Integrity

=

- Adobe
- NOKIA
- EMC^2
- symantec
- Juniper NETWORKS
- SAP
- Microsoft

No Effective Way to Prove Software Correctness



The Weak Link

Investing in Security

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?

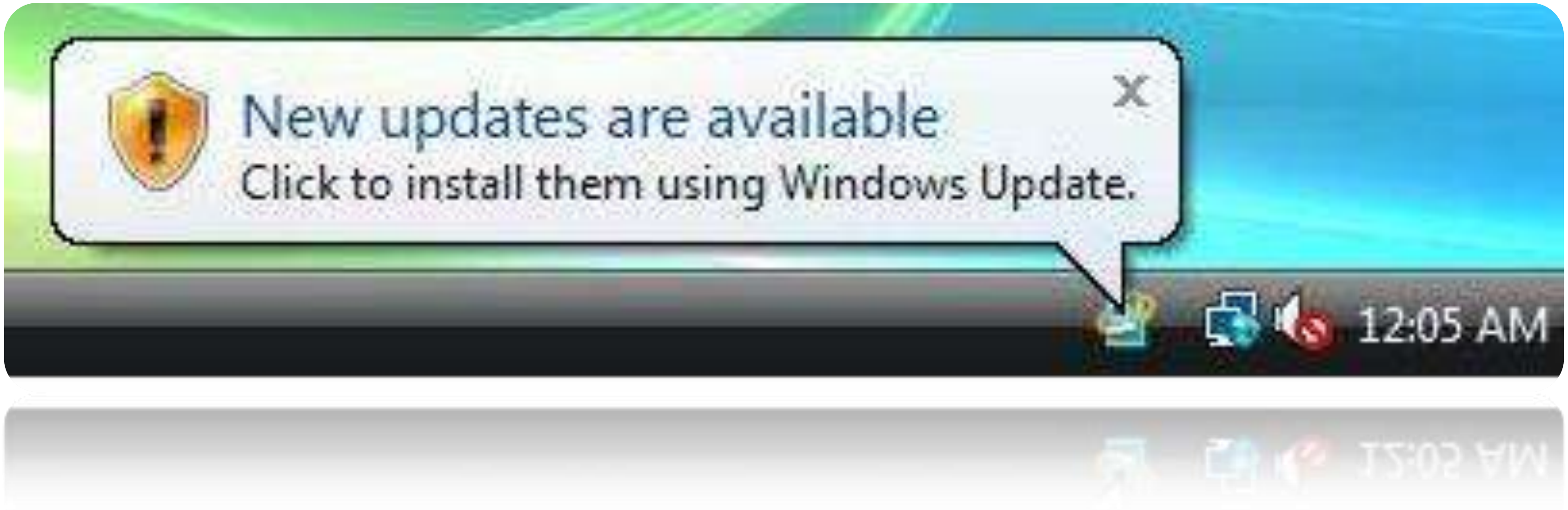
US$99,999

US$28,724

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?



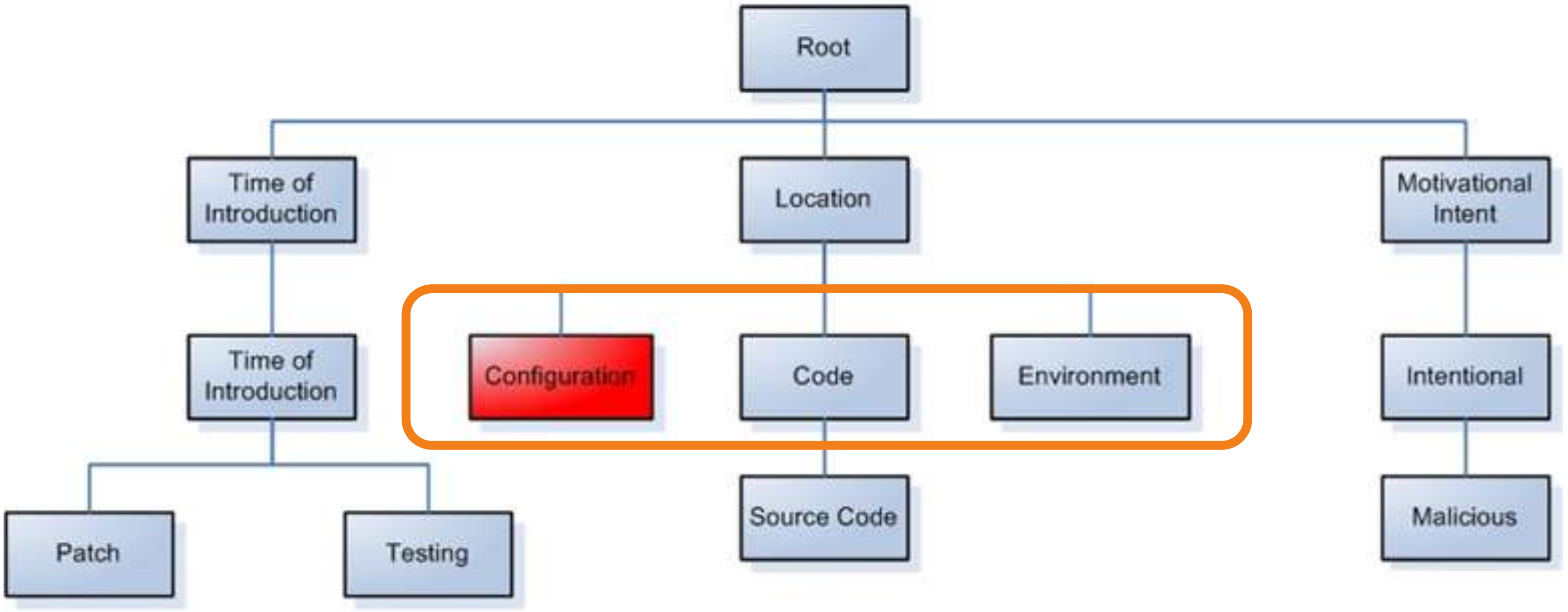
New updates are available

Click to install them using Windows Update.

Choosing to Adopt Software in Corporate Environments

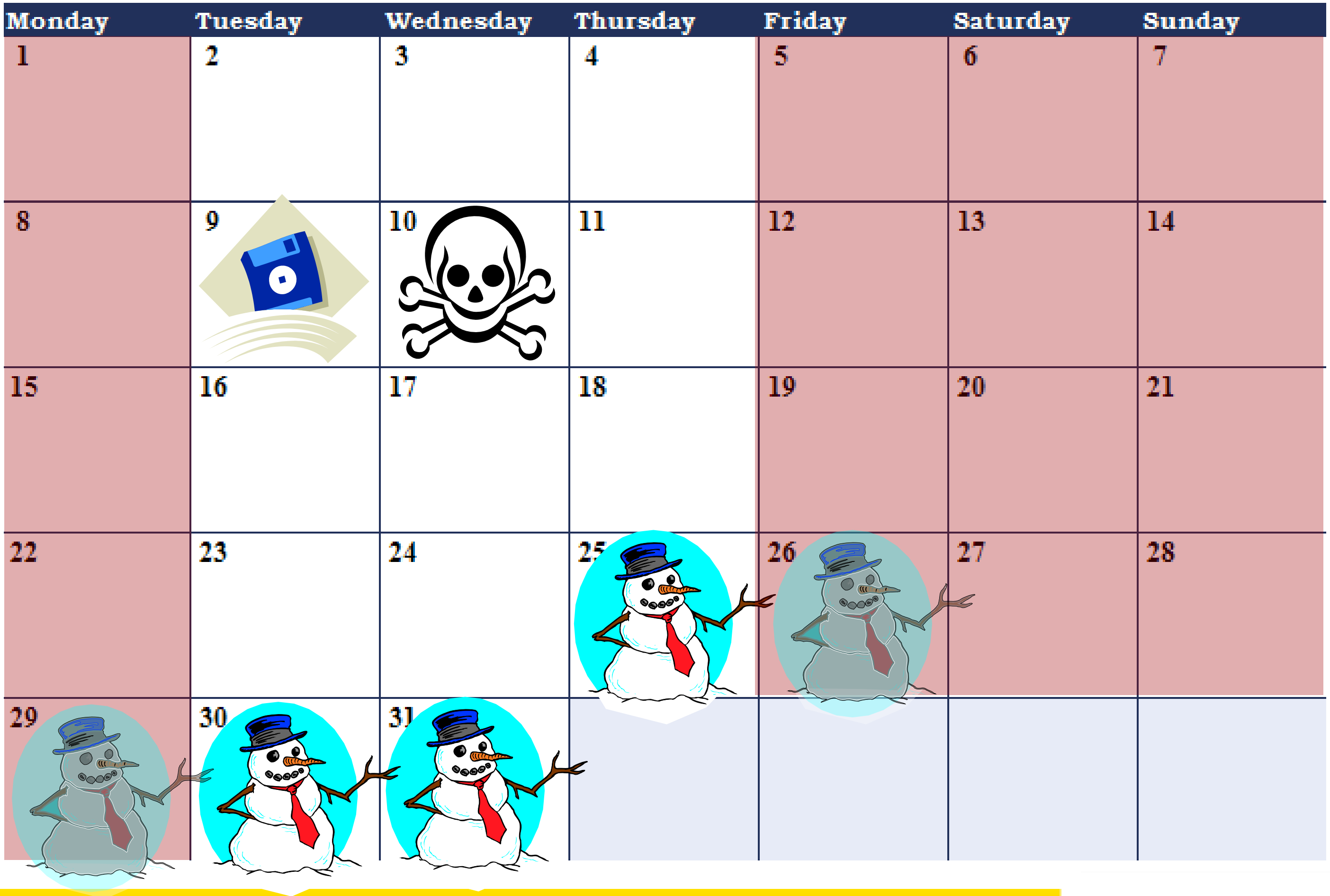
Weaknesses Can Come From Different Sources

Partial Representation of the CWE Tree



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

- **Motivation:** Fame, money, curiosity, ideal
- **Consequences:** full disclosure vs. responsible disclosure

Full Disclosure	Responsible Disclosure
Fame	Fame (and work)
Virus as a byproduct	Slower to provide a fix
Poor fixes (zero days), can use Firewalls for immediate protection	Better fixes

- **Incentives:** Vulnerability market
  - iDefense pay for *finding* vulnerabilities
  - Will it pay for *creating* vulnerabilities?
  - Will it *leak* information to increase the value of their subscription?

Government

Government

- Hard to create effective laws
  - Banning Hacking tools
  - Cutting Internet access of users spreading virus
- Certifications (code reviews)
- Using Government buying power to promote security
  - Federal Desktop Core Configuration (FDCC)
- Providing incentives
  - Treating vulnerabilities like pollution
  - Will it kill the small players?
- Cases that went wrong: USC vs. Eric McCarty
- Industry moves too fast, will laws be able to keep up with it?

Conclusions

Summary

- Economics play a larger role than technical solutions
- Industry is moving in the right direction
  - Small players will follow industry leaders
- Government does not necessarily understand the problem
  - Creation on laws can cause more damage than good
- The creation of a vulnerability market can have unintended consequences
- Users need to step up with their education

Thank you!

Cassio Goldschmidt

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)

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.