



# **Responsabilidade pelos Danos e Riscos Causados por Falhas de Segurança**

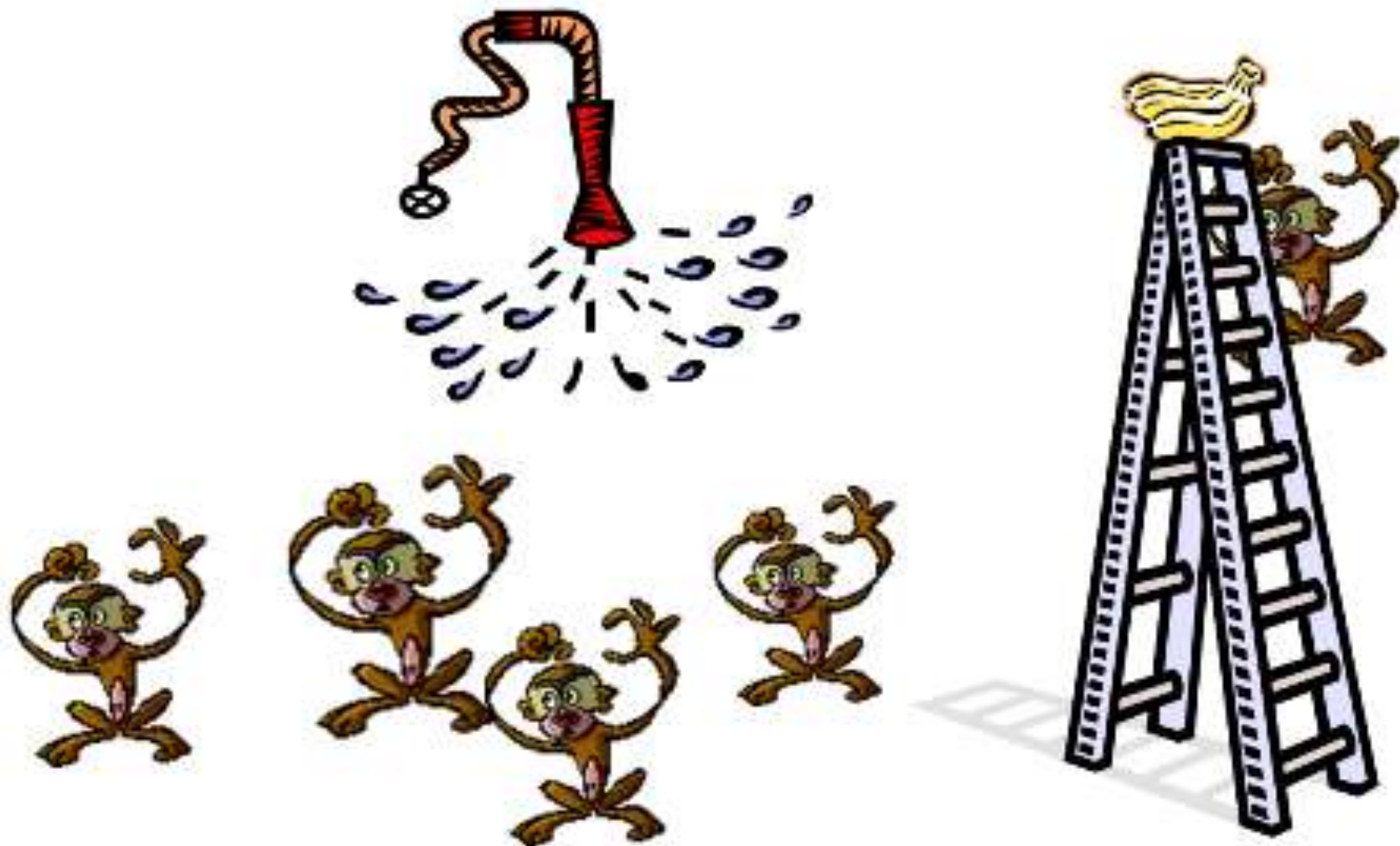
**Cassio Goldschmidt**

Gerente Senior, Segurança de Produtos

# O que é Software?

# Por que isso importa?!?!

# A Importância de Revêr Nossas Convicções



# Um Produto



# Um Serviço



# Um Discurso



# Um Bem Comum





# Bens Comuns Podem Ser Ruins



Responsabilidade pelos danos e riscos causados por falhas de segurança

**...e todos nós contribuimos para isso.**





# Agenda

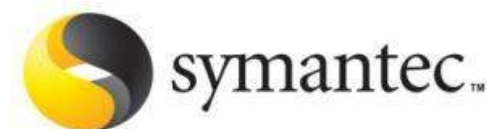


# Fabricantes de Software

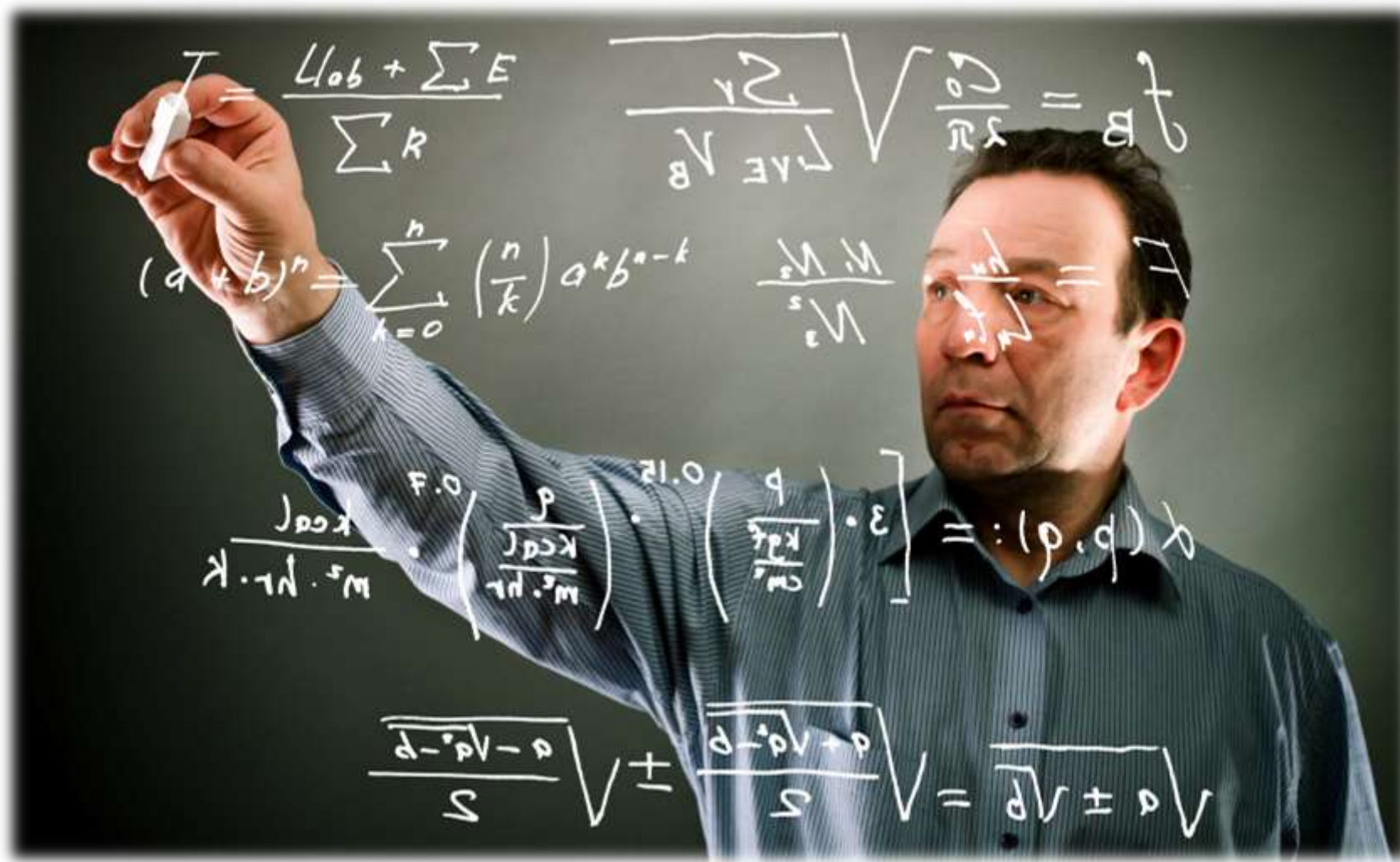
# Melhores Práticas em Segurança – SAFECode.org



=



# Como Provar que o Software está Correto?



# O Elo Mais Fraco



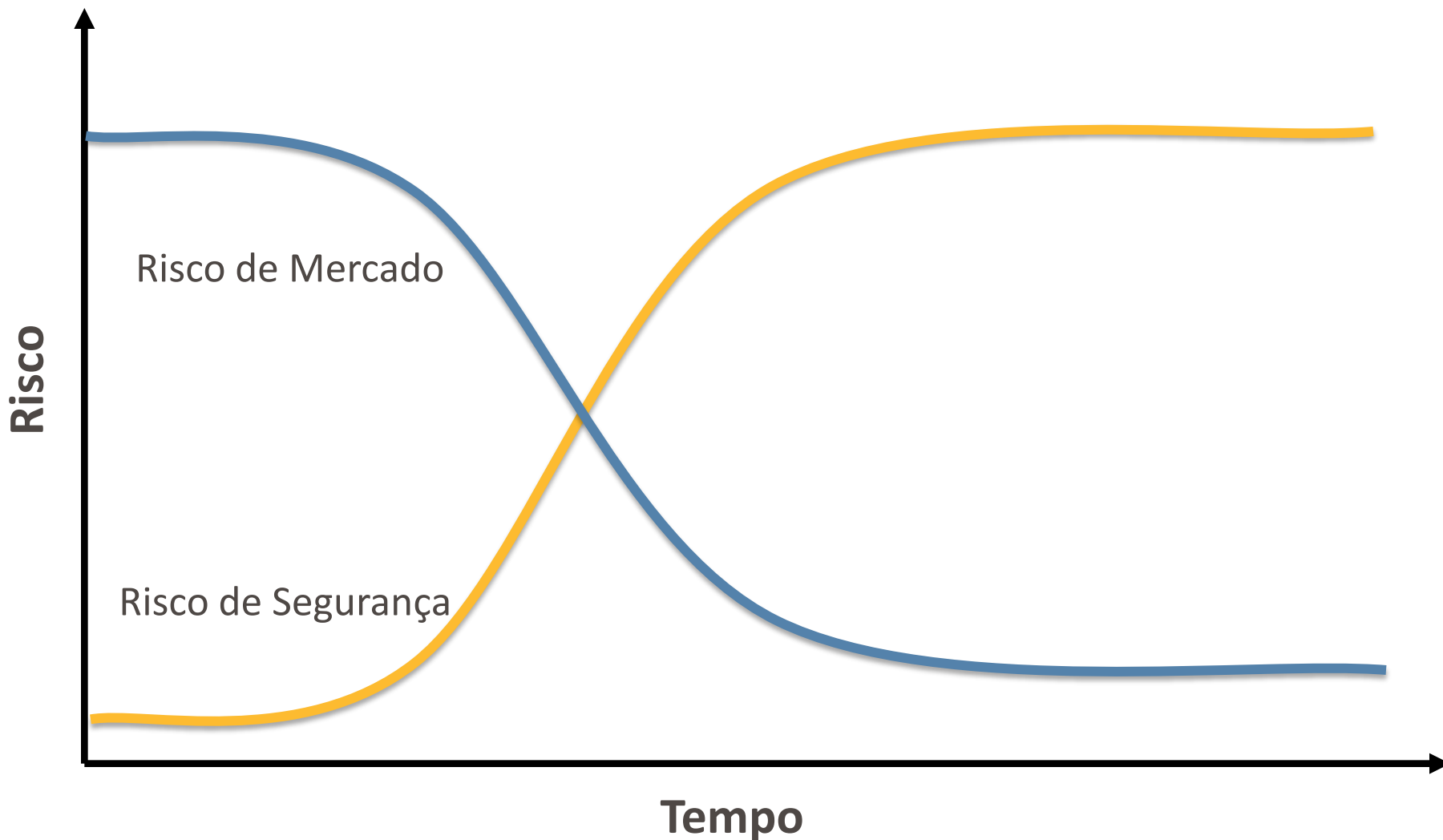


# Investimentos em Segurança





# Definição de Negócios da Palavra “Risco”



# Usuários Domésticos e Corporativos

# Usuarios Querem Funcionalidades

**US\$28,724**



- Confiável

**US\$28,724**



- Conversível
- Rodas de Liga Leve
- Aerofólio
- e Vermelho!

# Segurança não é Visível

Como os usuarios domésticos podem distinguir um produto seguro de um não seguro?



Security Facts		
Type: Web Application	Jun 28, 2010	
OWASP Top 10 2010		
A1-Injection		<input type="radio"/>
A2-Cross Site Scripting (XSS)		<input type="radio"/>
A3-Authentication		<input checked="" type="radio"/>
A4-Object References		<input type="radio"/>
A5-Cross Site Request Forgery		<input type="radio"/>
A6-Security Configuration		<input type="radio"/>
A7-Cryptographic Storage		<input checked="" type="radio"/>
A8-URL Access Control		<input type="radio"/>
A9-Transport Layer Protection		<input type="radio"/>
A10-Redirects and Forwards		<input type="radio"/>
Custom Code		
Name	Language	LOC
Core	Java	1200K
Developer Plugin	Java	20K
Reporting Page	Java	12K
Persistence Layer	PSQL	15K
User Interface	JSF	46K
Business Functions	Java	100K
Libraries		
Name	Language	H U
Struts 1.1	Java	<input type="radio"/> <input checked="" type="radio"/>
Log4j 1.0.3	Java	<input type="radio"/> <input type="radio"/>
ICM 2.1	Java	<input type="radio"/> <input type="radio"/>
Hibernate 3.0	Java	<input checked="" type="radio"/> <input type="radio"/>
OWASP ESAPI 2.0rc1	Java	<input type="radio"/> <input checked="" type="radio"/>
Platform Components		
Name	Language	H U
WebSphere 6.1.2	C/C++	<input checked="" type="radio"/> <input checked="" type="radio"/>
Java Enterprise Edition 3.1	Java	<input checked="" type="radio"/> <input checked="" type="radio"/>
Interfaces and Connections		
Name	Protocol	D E N Z
Web Interface	HTTPS	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
FTP Interface	FTP	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Google Search API	REST	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Syllux	TDS	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Oracle 11	SOAP	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Log Server	SNMP	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Mailbox	SMTP	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Sensitive Data		
Name	Contents	S T Z
Healthcare Records	CIA	<input checked="" type="radio"/> <input checked="" type="radio"/> <input checked="" type="radio"/>
Credit Card Numbers	CI	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
Application Security Program		
Practice	Provider	M
Strategy and Metrics	Internal	<input type="radio"/>
Policy and Compliance	Internal	<input type="radio"/>
Education and Guidance	Aspect Security	<input checked="" type="radio"/>
Threat Assessment	Internal	<input checked="" type="radio"/>
Security Requirements	Internal	<input checked="" type="radio"/>
Secure Architecture	Aspect Security	<input checked="" type="radio"/>
Design Analysis	Internal	<input type="radio"/>
Code Review	Aspect Security	<input checked="" type="radio"/>
Security Testing	Aspect Security	<input checked="" type="radio"/>
Vulnerability Mgmt	Internal	<input type="radio"/>
Environment Hardening	Internal	<input type="radio"/>
Operational Enablement	Internal	<input checked="" type="radio"/>
Security Contact: security@seccoresecurity.com		

# Efeito de Redes Afeta as Decisões

## Criação de um Ecosistema Afeta a Segurança



# Ignorar Atualizações de Segurança Afeta a Todos Nós

- Com qual frequência que você vê esta imagem nos computadores de seus amigos?



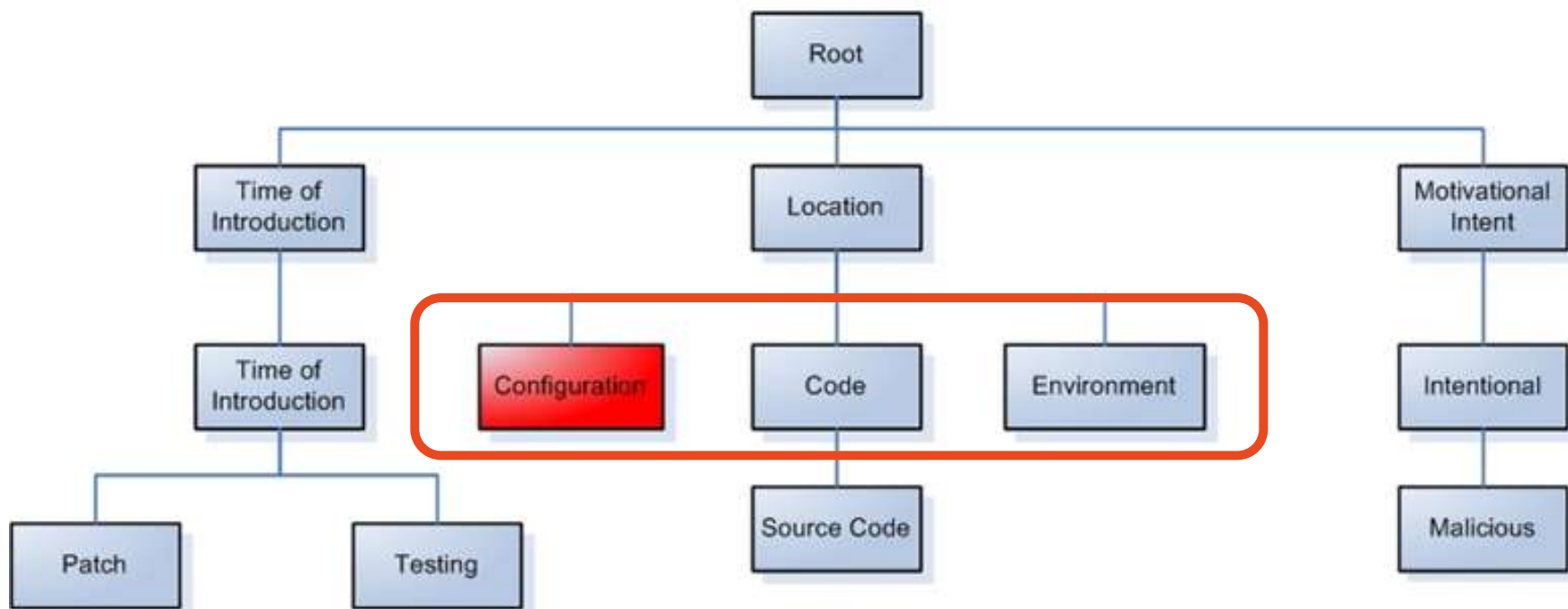


# Escolhendo um Software para Adoção em Ambientes Corporativos



# Fraquezas Podem Vir de Diversas Fontes

## Representação Parcial da Árvore CWE





# Congelamento de Atualizações

## Dezembro de 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 				

# Pesquisadores de Segurança

# Pesquisadores de Segurança



## Full Disclosure

- Todos os detalhes técnicos são revelados.

00:00

## Zero Day

- Detalhes técnicos são revelados antes do fabricante ser contactado.



## Coordinated Disclosure

- Descobridores de falhas e fabricantes de software trabalham juntos para achar uma solução.
- Nova encarnação de Responsible Disclosure

# Pesquisadores de Segurança

## Incentivos: Mercados de Vulnerabilidades



Pesquisador



Recompensa



Desenvolvedor



Crime

# Pesquisadores de Segurança

## Incentivos: Mercados de Vulnerabilidades



O que ocorre quando  
existe **vazamento** de  
informações?

# Governo

# Governo e a Criação de Leis

## Dificuldade de Criar Leis Eficazes





# Governo e a Criação de Leis Cortar Acesso a Internet









# Código Certificado

# Governo

## Tratando Falhas de Segurança como Poluição



Como ficarão as  
pequenas empresas?



# Governo Americano

## Federal Desktop Core Configuration (FDCC)



# Governo Muito Cedo para Fazermos Leis?







# 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](http://www.youtube.com/cgoldsch)

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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.