



# Responsible Vulnerability Disclosure

**Zoltán Précsényi**

Sr Manager Government Affairs EMEA

# Agenda

1

About Vulnerabilities

2

Responsible Disclosure: Industry Background

3

Responsible Disclosure: Symantec Policy

4

Public Policy Considerations

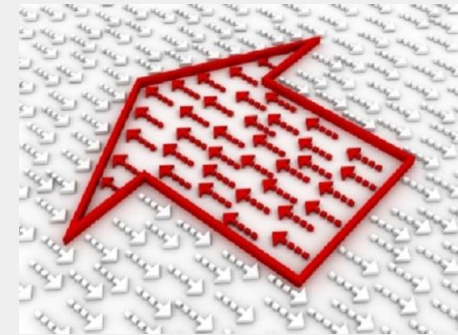


# About Vulnerabilities

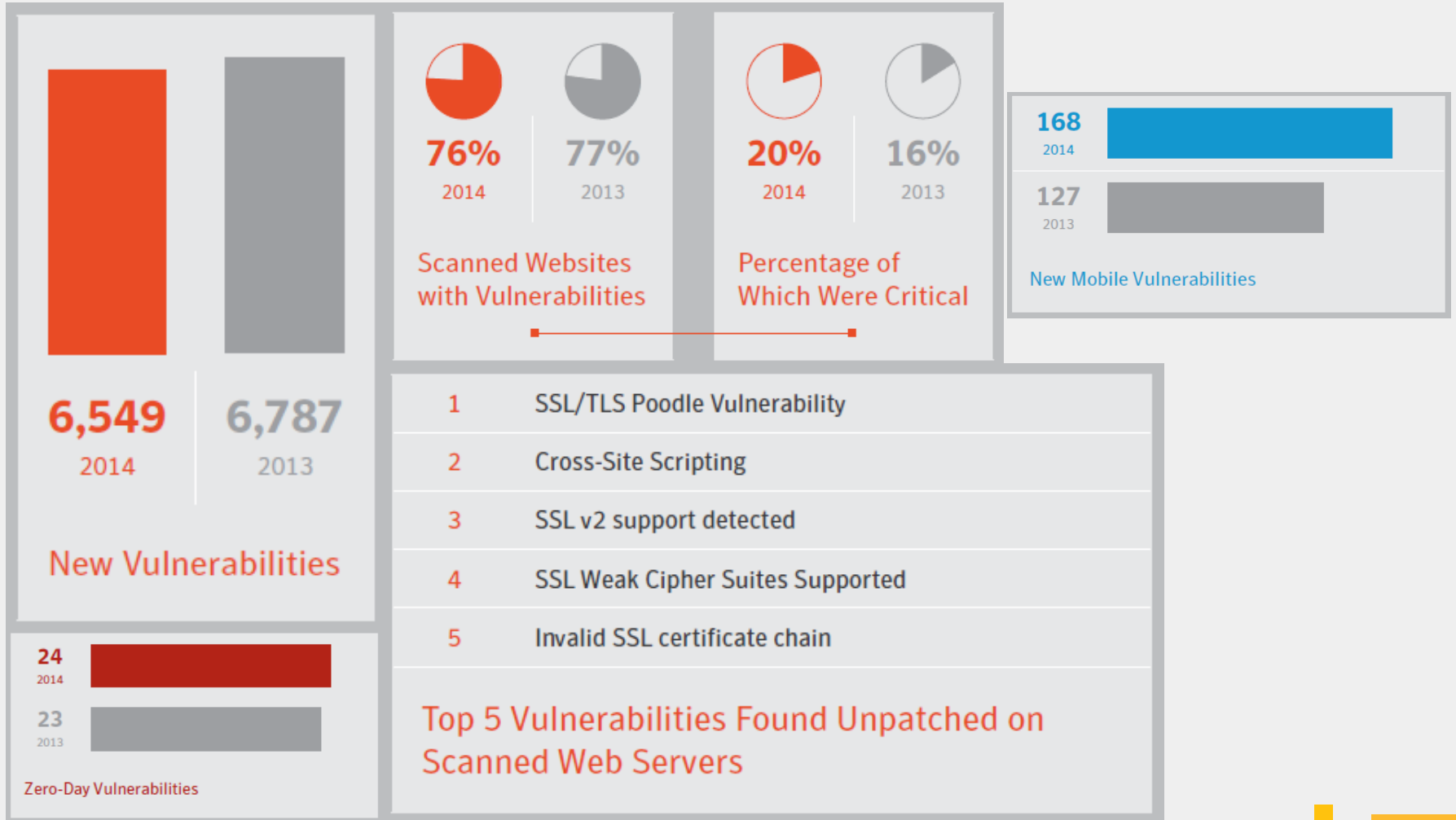
Latest Figures

# What Do We Call A „Vulnerability“?

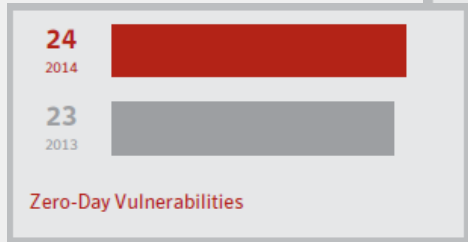
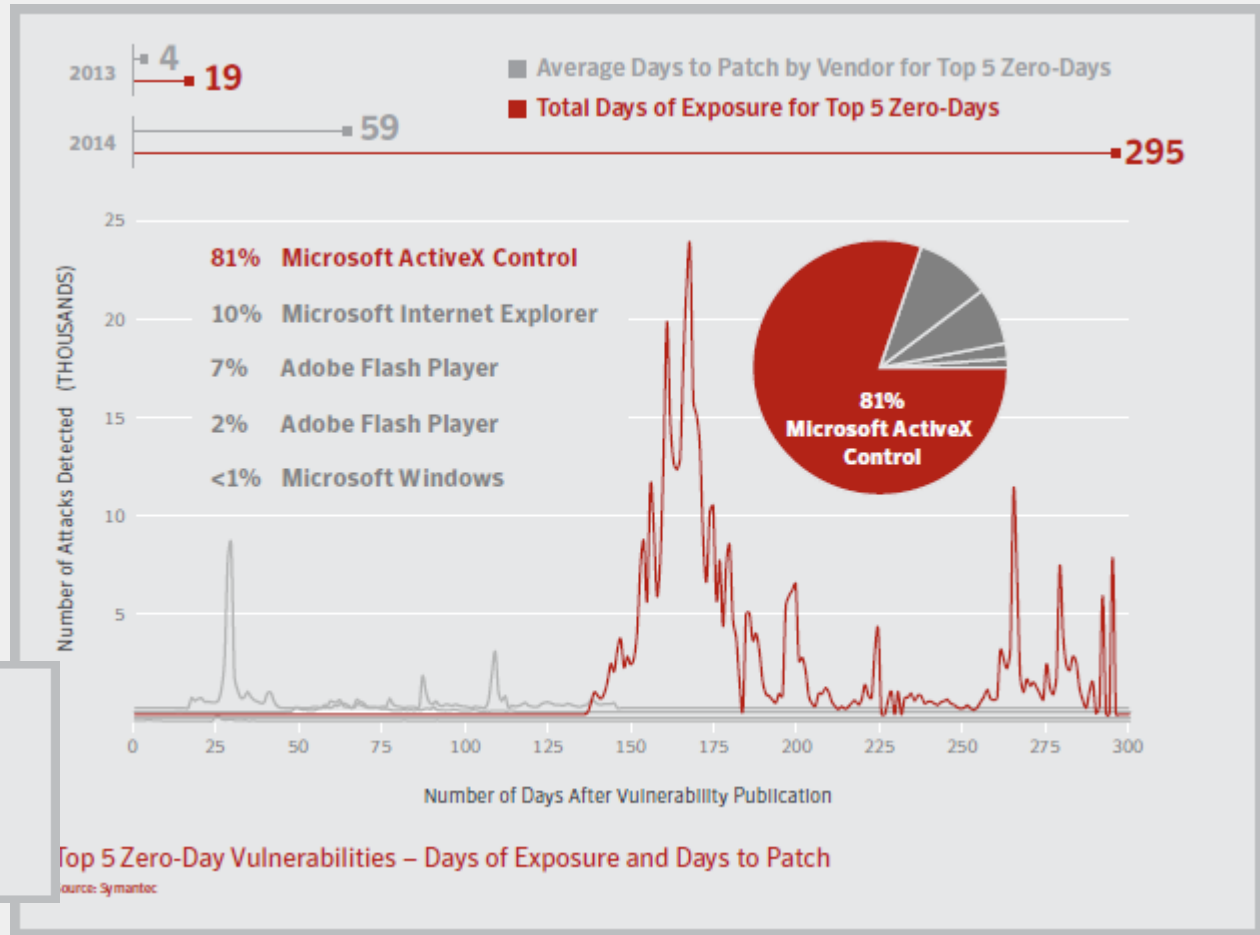
- **Flaw** within a **software** system...
- ...that can cause the system to **work contrary to its documented design.**
- It can allow attackers to:
  - **Execute** commands
  - **Access** data
  - **Pose** as another entity
  - **Deny** normally authorised access



# Vulnerabilities Recorded In 2014



# Zero-Days In 2014



# Security Advisories Published On Symantec Products

	2013	2014	2015 Jan-Apr
Unrated	-	1	-
Low*	-	1	-
Medium*	10	12	4
High*	2	3	-
<b>Total</b>	<b>12</b>	<b>17</b>	<b>4</b>

Source: [http://www.symantec.com/security\\_response/securityupdates/list.jsp?fid=security\\_advisory](http://www.symantec.com/security_response/securityupdates/list.jsp?fid=security_advisory)

**\* Ratings based on Common Vulnerability Scoring System Version 2.0 (CVSS-SIG):**

**Low:** Vulnerability unlikely to be exploited, to cause serious damage or to expose confidential information

**Medium:** Reasonable chance of exploitation, of moderate damage, of service disruption, or of exposure of confidential information

**High:** Very likely exploitation, serious damage, service disruption or target system compromise, and exposure of confidential information




# Responsible Vulnerability Disclosure

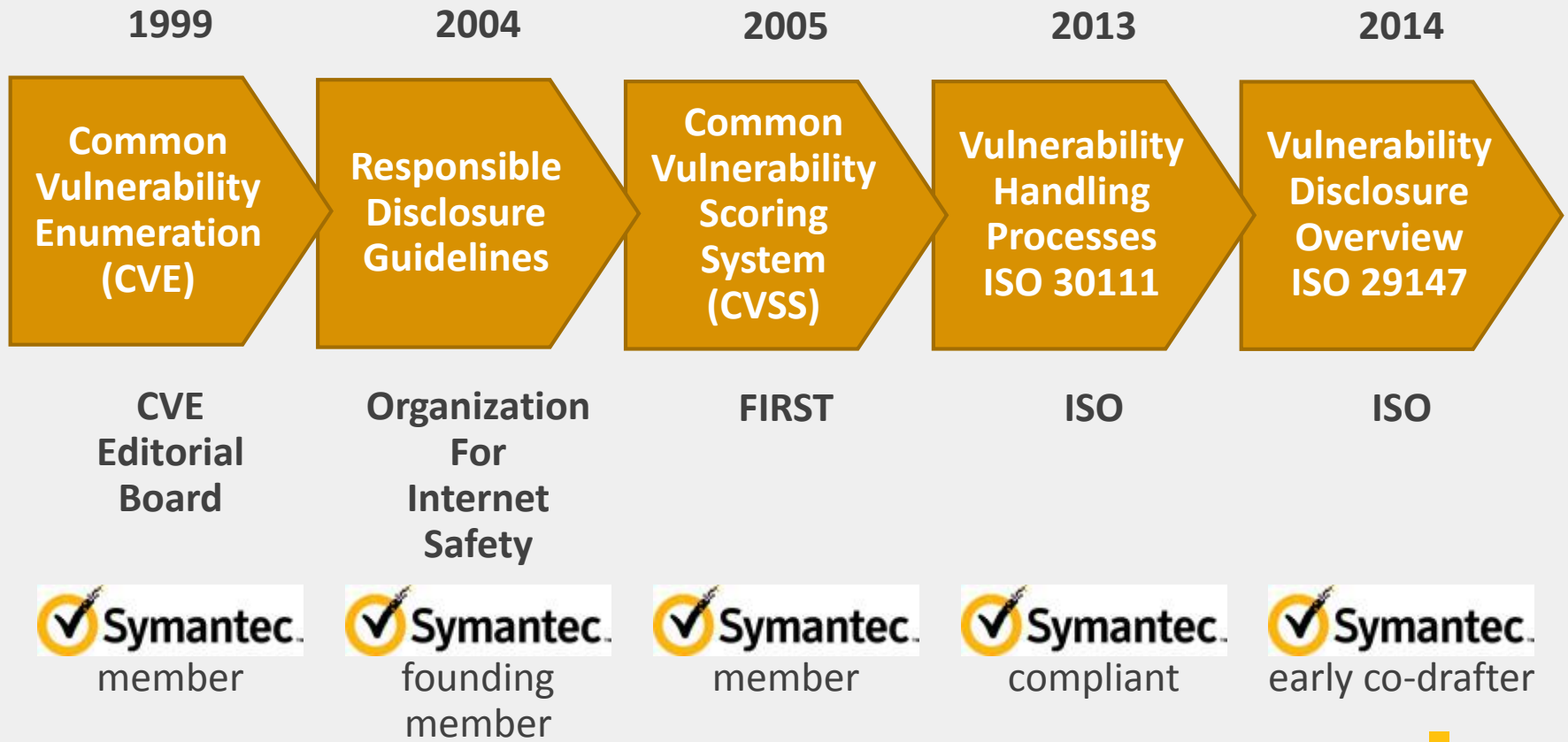
## Industry Background



# Available Disclosure Policy Options

	Full Disclosure	Responsible Disclosure	No Disclosure
<b>Main feature</b>	<ul style="list-style-type: none"> <li>• Full publicity upfront</li> </ul>	<ul style="list-style-type: none"> <li>• Carefully controlled and scheduled publicity</li> </ul>	<ul style="list-style-type: none"> <li>• No legitimate publicity</li> </ul>
<b>Upside</b>	<ul style="list-style-type: none"> <li>• Maximum public pressure on vendor</li> <li>• Reward to finders</li> </ul>	<ul style="list-style-type: none"> <li>• Early handling by authorised experts only</li> <li>• Reasonable exposure control</li> </ul>	<ul style="list-style-type: none"> <li>• No lawful broadcasting to malicious players</li> </ul>
<b>Downside</b>	<ul style="list-style-type: none"> <li>• Gives blueprint for attackers</li> <li>• Incentivises race to hack</li> </ul>	<ul style="list-style-type: none"> <li>• Relies on finder and vendor diligence</li> <li>• Dependent on patch hygiene</li> </ul>	<ul style="list-style-type: none"> <li>• Doesn't stop black market</li> <li>• Leaves all legit players in the dark</li> <li>• Doesn't reward good practices</li> </ul>
<b>Assessment</b>	<b>Highest Risk, Undesirable</b>		<b>Neither realistic, nor desirable</b>

# The Existing Framework Of Responsible Disclosure





# Responsible Vulnerability Disclosure

## Symantec Vulnerability Management Policy

# Symantec Vulnerability Management: Basic Facts

- **History:** Vulnerability Management Team created 15 years ago
- **Continuity:** The same manager has been in place ever since
- **Engagement:** Active in relevant fora since the start
- **Governing Principle:** Responsible Disclosure

# Symantec Vulnerability Management: The Approach

## Prevent

**Responsible Product Development**

**Secure Coding education of staff**

**SAFECODE engagement**

**Testing, auditing, certification of products as and when appropriate**

## Detect

**Receive finders' notifications**

**Review and assess vulnerability and threat**

**Determine affected products and relevant course of action**

## Respond

**Research extra information to rate severity**

**Develop and thoroughly test patches**

**Deploy correction and mitigation measures**

**Publicise product security advisory**

# Symantec Vulnerability Management: The Process

## INITIAL CONTACT

- Through public email address: [secure@symantec.com](mailto:secure@symantec.com)
  - Using a PGP public key available to finders
  - Including all relevant info the finder can provide

## PRELIMINARY EVALUATION AND ACKNOWLEDGEMENT

- Initial review and acknowledgement to finder
- Request to the finder for additional information for validation
  - Validation of the finding

## VULNERABILITY EVALUATION

- Distribution to all relevant product groups and software security engineers
- Validation of the vulnerability and determination of supported products affected
  - Request to the finder for additional information to reproduce the issue

## COORDINATION WITH FINDER

- Communication of the vulnerability and threat evaluation to the finder
  - Plan of action for patch development, testing and deployment
  - Preparation of the release of public communications

## PUBLIC NOTIFICATION

- Release of a Symantec Product Security Advisory
- Coordination of advisories from other parties (finder, third party vendors)
  - Full credit to the finder

Single Point of Contact and Coordinator Throughout:  
Symantec Software Security Vulnerability Manager

# Symantec Vulnerability Management: FAQs

- **Resolution Timeline:** No set timeline because every case is complex and different.
- **What causes complexity:** Every case comes with unique needs for investigation, resolution, localization, testing.
- **Prioritisation:** Based on severity and urgency. Round-the-clock operation in case of serious vulnerabilities.
- **Patching:** Industry benchmark from release to deployment is 30 days, but this depends largely on the user.
- **User responsibility:** Vendor cannot intrude into user systems.
- **Finder responsibility:** Responsible Disclosure only works to the extent that finders themselves abide by its rules and principles.
- **Bug bounty:** Symantec doesn't give any so as not to engage into bidding against the underground market, but fully and publicly credits finders.
- **Third party vulnerabilities:** Symantec abides by all the rules and principles of Responsible Disclosure in all circumstances, both as affected vendor and as finder.



# Responsible Vulnerability Disclosure

## Public Policy Considerations



# Public Policy Considerations To Bear In Mind (1)

- **Is the current Responsible Disclosure industry practice good enough?**  
Symantec considers it as the state of the art.
- **Legislate vulnerability disclosure or not?**  
Reflect carefully on what you want to achieve and whether the measures you envisage will actually achieve it.
- **Mandate disclosure?**  
Don't give cybercriminals the blueprint to attack you.
- **Mandate disclosure after a reasonable period?**  
What's reasonable? What if the vulnerability is not fixed? What if the product is no longer supported? What if the vendor no longer exists?
- **Require restricted disclosure to public authorities such as NIS agencies and Gov CERTs?**  
Which ones, in what case, to what end? Responsible Disclosure works so far as trust is upheld and the need-to-know principle is applied between the finders, vendors and legitimate users, be they public or private.

## Public Policy Considerations To Bear In Mind (2)

- **Make vendors liable for vulnerabilities in their products?**

Technological evolution + complexity → zero risk doesn't exist.

Vendor liability wouldn't deter attacks, but it could freeze development.

- **Make vendors liable for patch deployment?**

That could only work if vendors could intrude into their customers' privacy.

- **Make vendors liable for not fixing vulnerabilities?**

How do you make such a determination fairly? How do you gauge such a liability? How do you enforce it? Upon reflection, an amendment to this effect was dropped from Directive 2013/40/EU.

- **Criminalise the non-responsible disclosure or trade in vulnerabilities?**

If it qualifies as aiding and abetting, it is already criminalised. Beyond that, be careful not to deter legitimate security research.

- **Go for Open Source?**

From a security standpoint, Open Source is neither superior nor inferior to proprietary technologies. Symantec builds on both. Having said that, if everyone's in charge, who's responsible?



# Q&A



Thank you!

Zoltán Précsényi

[zoltan\\_precsenyi@symantec.com](mailto:zoltan_precsenyi@symantec.com)

+32 225 71 319

**Copyright © 2015 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.