Reporting Security Vulnerabilities: Defining Best Practices For Industry & Third Party Co-Ordinators

Presented by:
Tara Flanagan
Director, Legal Services
Cisco Systems, Inc.
tflanaga@cisco.com
January 2006

Reporting vulnerabilities is like ……..

Agenda

- Assumptions & Criteria
- The Discovery Phase
- The Pre-Public Announcement Phase
- The Security Publication Phase
- The Post-Announcement Phase
- Wrap Up

Baseline Assumptions for a Co-ordinated Reporting Process

- It is in the long term interest of industry and government to have a public vulnerability reporting process.
- Co-ordinators play a key role in reporting vulnerabilities that impact multiple vendors' products.
- The reporting process has to be worldwide (Internet has no regional barriers).

Foundational Best Practice Criteria
For Both Industry and Third Party Co-ordinators:

- A firm commitment to a public reporting process.
- A dedicated team (24x7/365).
- An empowered team, with ability to make key decisions quickly and act.
- A team that is independent from other internal organizations who may have conflicting interests.
- A written, published policy regarding their security reporting/co-ordination process.
- A recognition of the different phases of the reporting process, which will implicate various activities and standards of care for all involved.
- A desire to continually drive to improve the overall process.

The Discovery (Pre-Reporting) Phase

The Clock is Now Ticking ……

Best Practices require that:

- Vendors commence actions to verify, define, scope and develop fixes and work-arounds for a discovered (but not yet public) vulnerability.
- Co-ordinators commence actions to set time for public reporting/handle other matters.
- Both vendors and co-ordinators undertake diligent efforts to maintain confidentiality = avoid exploitations.

Maintaining Confidentiality Is Key

Best Practice: How to internally manage in any organization:

- Adopt a process that reminds personnel of their confidentiality obligations and that keeps track of who has access to the sensitive information.
- Be prepared to, and do, enforce any internal breaches.
- Share information internally on a strict *need to know* basis.
- Establish separate communication tools/email aliases.
- Have separate walls for your security reporting team.

Activities that Can Impact A Co-ordinated and Scheduled Public Disclosure of a Vulnerability

- Private contracts between customers and vendors that would require pre-disclosure.
- Regional laws that would require pre-disclosure.
- Intentional disclosures by independent researchers/third parties.
- Inadvertent disclosures.

What should be the "best practice" contingency plans for co-ordinators and participating vendors if any of the above happen?

Pre-Public Announcement:

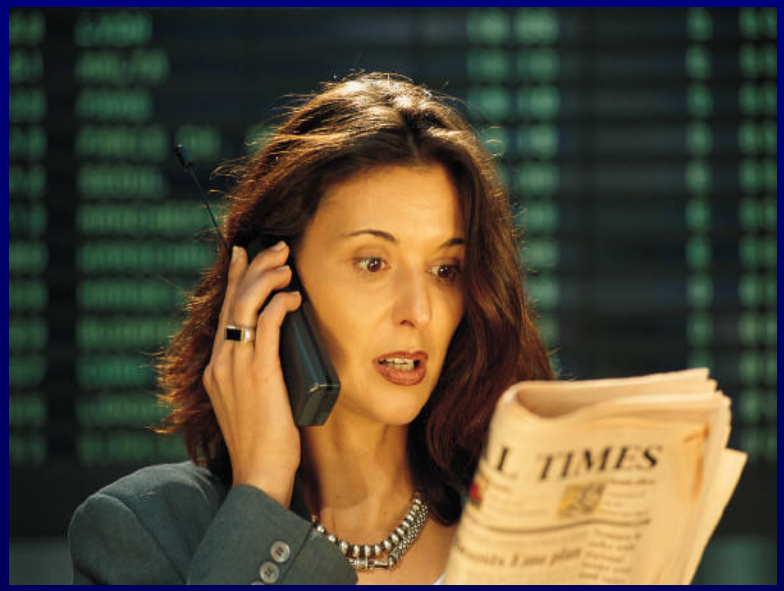
- Determining the timing of public posting of security advisories (world wide): What are key factors? What factors should not be considered?
- Review Process of Draft Advisories.
  Who/how many people should review and what kind of a process do you use?
- Substance of the Advisories: How do you ensure consistency/word usage? What kinds of words should be avoided? What languages to use? Problems with translations?
- Preparing accompanying public statements for media post-disclosure.

The Security Announcement Itself

- Factual content only-no spin.
- Clear instructions/information.
- Avoid unnecessary detail that might cause/contribute to an exploit.
- Placement of the announcement on your web site: Can you find it easily?
- Do you make it easy for the reader to reach you if they have questions?
- Do you provide a way for the reader to give you immediate feedback on the advisory?

Post-Announcement Issues

- Preparing for Consistent Customer/Public Communications
- Responding to press releases/communications: how respond without appearing defensive.
- The value of post-mortems



Wrap Up

- Reporting landscape is increasingly complex.
- Uncertain: Future impact of world wide legislative/regulatory/enforcement activities to address concerns regarding security, ecommerce and data privacy.
- What is certain: Reporting security vulnerabilities today cannot be ad hoc: Companies and third-party co-ordinators should continue (through FIRST/other industry groups) to define, publish, advocate and follow best practices.

Best Practices=More Consistent, Effective Reporting Process

Q and A