

Canadian IT Managers

 Broadly Connecting Canadian IT managers through Career, Industry, and Technology insight

Dec January 2006 Feb

S	M	T	W	T	F	S
25	26	27	28	29	30	31
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	1	2	3	4

My Links

- [RSS 2.0](#)
- [Atom 0.3](#)
- [Contact](#)

Search

 [Go](#)

Archives

- [January 2006 \(23\)](#)
- [December 2005 \(26\)](#)
- [November 2005 \(8\)](#)
- [October 2005 \(6\)](#)
- [September 2005 \(2\)](#)
- [August 2005 \(7\)](#)

News

For me sharing of thoughts and information is what blogging is all about. This way we can learn from each other.

These postings are provided "AS IS" with no warranties, and confers no rights. You assume all risk for your use.

» [Blogs that link here](#)

 Technorati



Canada's Association of Information
Technology (IT) Professionals

Resident Bloggers

[Stephen Ibaraki](#) Technology Journalist I.S.P., DF/NPA, CNP

[John Oxley](#) Director IT Pro Evangelism
Microsoft Canada

[Barnaby Jeans](#) IT Pro Advisor
Microsoft Canada



Navigation

- [Home](#)
- [Blogs](#)

Post Categories

- [Industry Perspectives \(rss\)](#)
- [MS News \(rss\)](#)

A Development Process Model for More Secure Applications

You hear about security all the time but have you and your team been designing your applications with security in mind. I found this web-cast, "5 Steps for Developing Secure Applications," from ITworld.com dated January 12, 2006 provides a good overview roadmap for IT managers:

http://www.accelacast.com/webcasts/gartner_compuware_app/

A synopsis of the web-cast's main themes follow:

Essentially 75% of security hacks occur at the application level however application security dealt with throughout the whole development lifecycle has not traditionally been a priority of developers. A key is for developers to think about application security as a defect and use the same processes that are used to find other defects. A good rationale is that hackers will not tell you about security defects like the way customers typically talk about other application defects. So developers need to track security vulnerabilities as defects and Operations needs to assess the risk of known defects. Moreover, QA must include security testing; applications must meet legislation requirements and not be susceptible to litigation. And applications must meet internal and external [partner] auditing requirements.

5 steps for Developing Secure New Applications include:

- 1) Assess business risk: legal, lost revenue, lost productivity, damage to brand, internal apps data exposure
- 2) Start with architecture: training for threats model, minimize damage
- 3) Code securely
- 4) Test early, test often
- 5) Validate for security: think like a hacker, focus on mal-formed data

3 steps for Assessing the Security of Existing Applications:

- 1) Assess vulnerabilities
- 2) Business risk assessment
- 3) Fix critical defects first

Thank you,
Stephen Ibaraki

posted on Monday, January 23, 2006 9:00 AM by [cdnitmgr](#)

[Post a Comment](#) ::

Comments