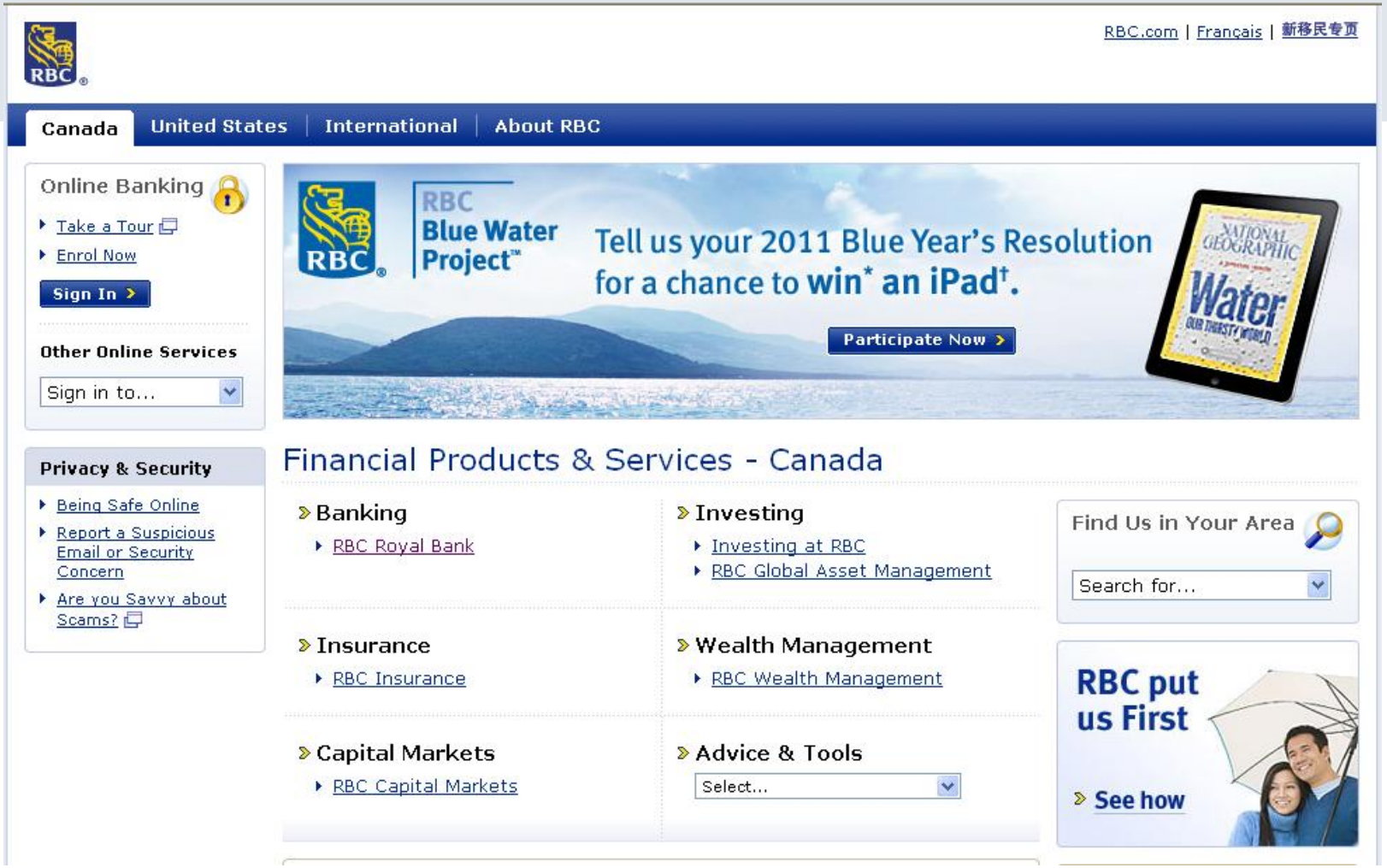
How Real World Software Security Programs Work

'How has your program evolved over time?'

SANS What Works In Application Security Summit
March 2011

INFORMATION SECURITY

About RBC


RBC.com | Français | 新移民专页
Canada
United States
International
About RBC
Online Banking
Take a Tour
Enrol Now
Sign In
Other Online Services
Sign in to...
Privacy & Security
Being Safe Online
Report a Suspicious Email or Security Concern
Are you Savvy about Scams?
RBC Blue Water Project™
Tell us your 2011 Blue Year's Resolution for a chance to win* an iPad†.
Participate Now
Financial Products & Services - Canada
Banking
RBC Royal Bank
Investing
Investing at RBC
RBC Global Asset Management
Insurance
RBC Insurance
Wealth Management
RBC Wealth Management
Capital Markets
RBC Capital Markets
Advice & Tools
Select...
Find Us in Your Area
Search for...
RBC put us First
See how

Where We Started

- Program staffed with Project Manager
- Sourced consulting help
  - Training materials & delivery
  - SDLC integration assistance
- Bought tools, expensive ones, and didn't use them effectively
- Voluntary use of tools for code review
- Professional services to test external sites

Hire Developers

- **Ability to work 1:1 with developer peers**
  - **Awareness and consulting**
  - **Hands on guidance with tool usage**
  - **‘Making the problems real’**
- **Tool-assisted static code analysis**
- **Pen testing**
- **Training**

Make it Mandatory!

- Volunteer program was an abject failure
- Problem statement not well understood
- Cost and time pressures an additional barrier to adoption
- Software security deliverables built in to SDLC
- Deployment of achievable objectives
- Risk based approach

Train, Train, and Train Some More

- **Spent a lot of time looking for the perfect training - pretty good *is* good enough**
- **CBT is a crucial tool**
- **Hands-on experience key for early adopters**
- **Presentations, seminars, user groups are all opportunities to get the message out**
- **Videos, checklists, user guides**

Where Do We Go From Here?

- **Metrics and Reporting**
- **Ensuring security of outsourced development**
- **Effective management of Open Source vulnerabilities**

Contact

Greg Ruddell

Director – Application Services

Information Security

RBC

greg.ruddell@rbc.com

(416) 348-4602

INFORMATION SECURITY