How to Get Along with Vendors Without Really Trying

A Guided Tour for Hackers on Current Vendor Disclosure Policies and Upcoming Standards

Katie Moussouris
Senior Security Strategist Lead, Microsoft Security Response Center
Microsoft Corporation

Agenda

- Intro – Who, Why, What
- Vulnerability Disclosure – Know Your r00tz
- Online Services Vulnerability Disclosure
- Ways to Make some Legit $$
- ISO Standards are Your Friends (really)
- Summary
- Questions

Who Mom Loves

- Joined Microsoft in April 2007
- Now I run Microsoft Security Community Outreach & Strategy, MSVR, and BlueHat ☺
- My (Security*) Work in Bullet Points:
  - Linux Dev and Security Tzarina - TurboLinux, circa 2000
  - Pen Tester - Artist formerly known as @stake
  - Founder - Symantec Vulnerability Research (SVR)
  - Founder - Microsoft Vulnerability Research (MSVR)
  - Policy Maker
    - Editor for draft ISO standard on Vulnerability Handling (30111)
    - Lead SME for US National Body on Vulnerability Disclosure (29147)

* Was a molecular biologist in a past professional life, worked on the Human Genome Project

Why Try to Get Along with Vendors?

- Karma
- Opportunities for You
  - Compensation (Money)
  - Reputation (Fame)
  - Influence (Power)
- Life is Too Short to Fight (with Some Vendor)

A Brief History of Disclosure

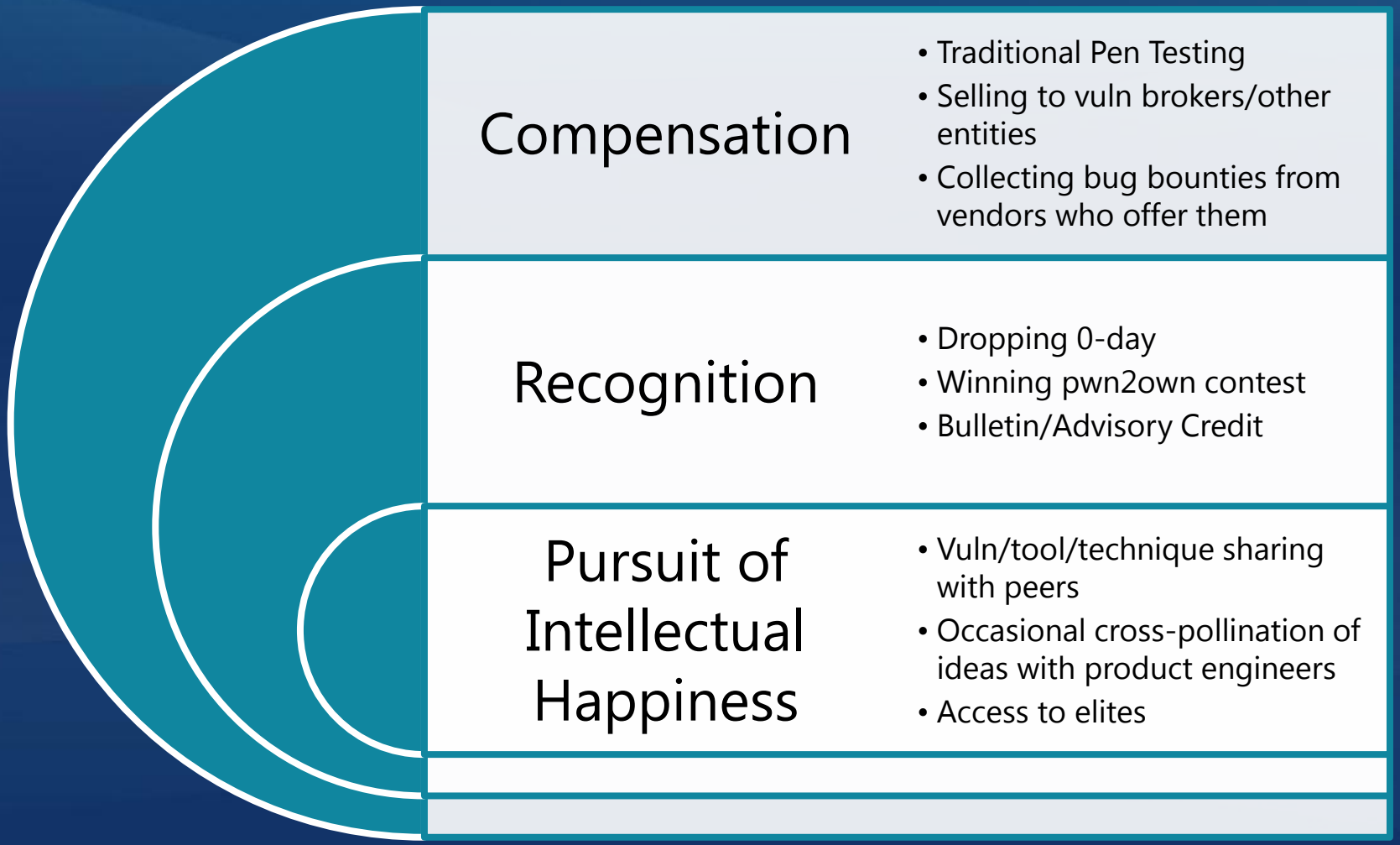
- Rain Forest Puppy's RFPolicy circa 1999
- Murky Origins of the term "Responsible"
- Org for Internet Safety and NIAC Guide circa 2004
- ISO standard study period on "Responsible" Disclosure Standard November 2006
- Jake Kouns (OSF) suggests the term "Coordinated" to me instead in February 2010
- ISO drops "Responsible" from the draft standard in April 2010
- Microsoft changes to "Coordinated Vuln Disclosure" in July 2010
- Microsoft's CVD process (as finder, coordinator, and vendor) is released in April 2011
- ISO standard on Vulnerability Disclosure should be **published circa Fall of 2013**

Online Services Vuln Disclosure

- July 2007 - Microsoft issued the first statement of any major vendor, pledging not to pursue legal action against researchers who privately report online service vulns
- PayPal follows shortly, but EXCLUDES brokered vulns from their exemption
- More recent vendor policies from Google, Facebook, etc. pledging amnesty
- Laws vary – check with a lawyer in your country!
  - e.g., CFAA in US
- Vendors vary – find their posted policy before you begin testing, verify with the vendor if you're not sure!

So What's In It For Researchers?

Pre-2012 Researcher Motivations/Fulfillment



The Vulnerability Economy

White Market

- Vendor Bug Bounties and brokers who share vulns with vendors
- Info used for defense
- Prices in the range of $500 - $60,000

Grey Market

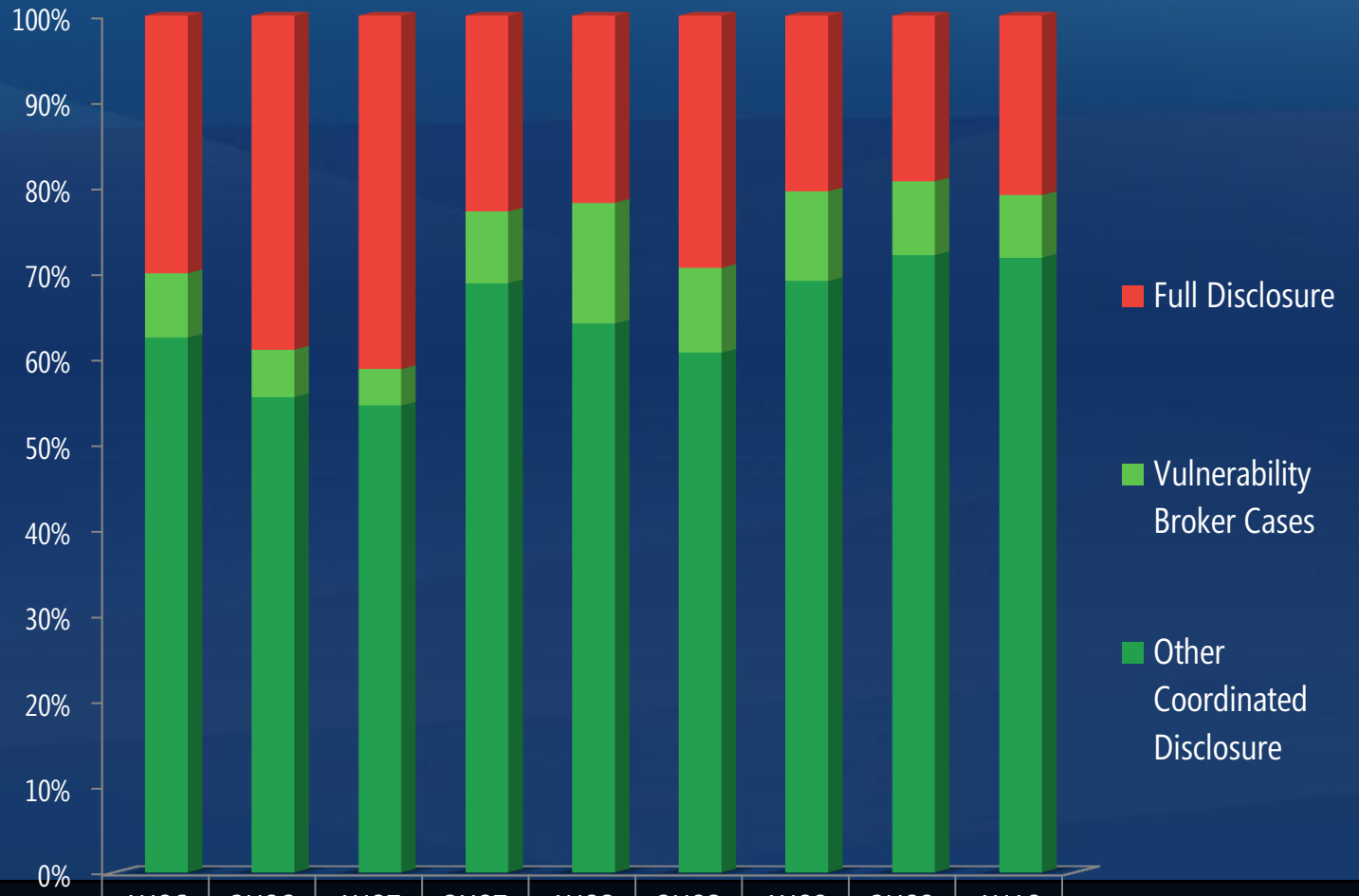
- Brokers who don't share vulns with vendors
- Info used for defense and offense
- Prices in the range of > $20,000

Black Market

- Governments and Organized Crime buyers
- Info used for offense
- Prices reported as great as >$1M

The White Market Does Not Compete With the Other Markets
The Price Increases Depending on the Vulnerability's Intended Use

Microsoft Vulnerability Details
Coordinated Vulnerability Disclosure Rates



	1H06	2H06	1H07	2H07	1H08	2H08	1H09	2H09	1H10
Full Disclosure	100	169	164	82	110	128	80	101	86
Vulnerability Broker Cases	25	24	17	30	71	43	41	45	30
Other Coordinated Disclosure	208	241	217	247	323	264	270	377	295

The Vulnerability Economy and You (and MS)

Researchers in general	• Have other motivations besides money
Researchers who report vulnerabilities to Microsoft	• Over 90% of private reports are made directly to Microsoft

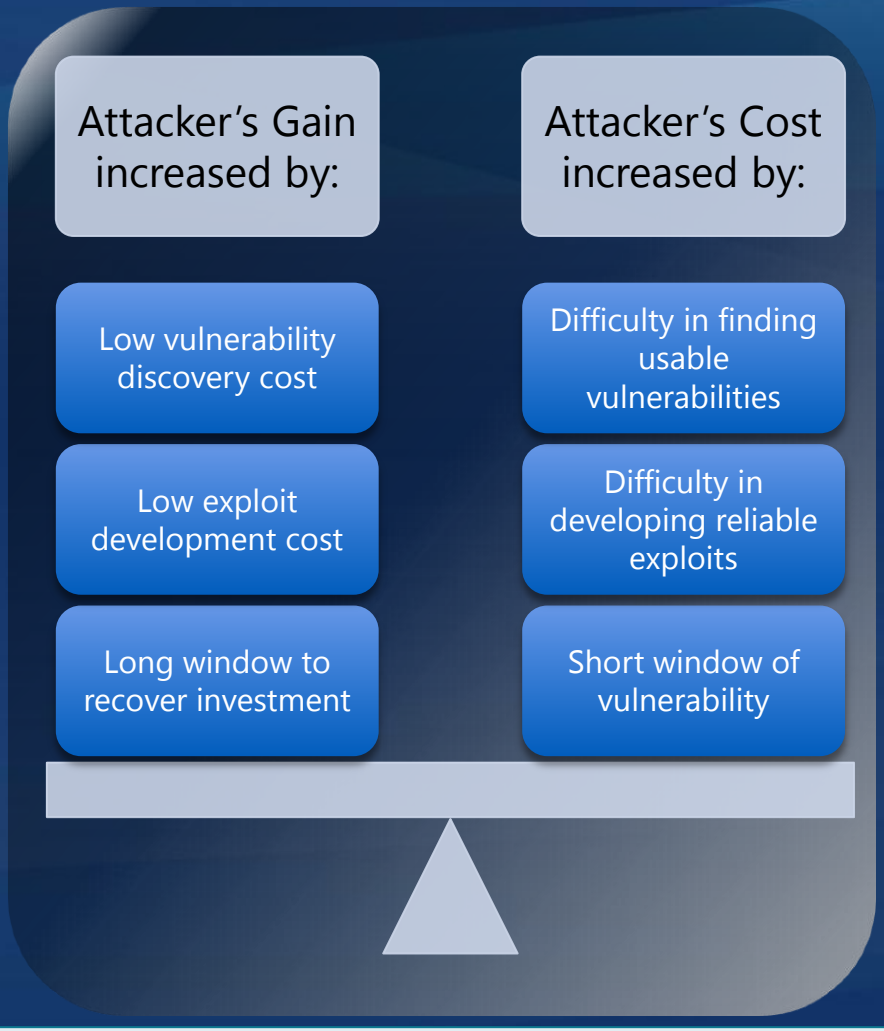
- We respect researchers' right to earn a living from their work
- We hope researchers who sell vulnerabilities choose the white market
- We try to hire talented researchers to help us improve our security

BlueHat Prize Announcement

- **First BlueHat Prize Challenge:**
  - Design a novel runtime mitigation technology that is capable of preventing the exploitation of memory safety vulnerabilities
- **Entry Period:** Aug 3, 2011 – Apr 1, 2012
- **Winners announced:** BlackHat USA July 2012
- **IP remains the property of the inventor**, with a license for Microsoft to use the technology

Grand Prize:	• **$200,000** in cash
Second Prize:	• **$50,000** in cash
Third Prize:	• **$10,000** in cash

Exploit Economics



Increase investment to find vulnerabilities

- Remove entire classes of vulnerabilities where possible
- Focus on automation to scale human efforts

Increase investment to write exploits

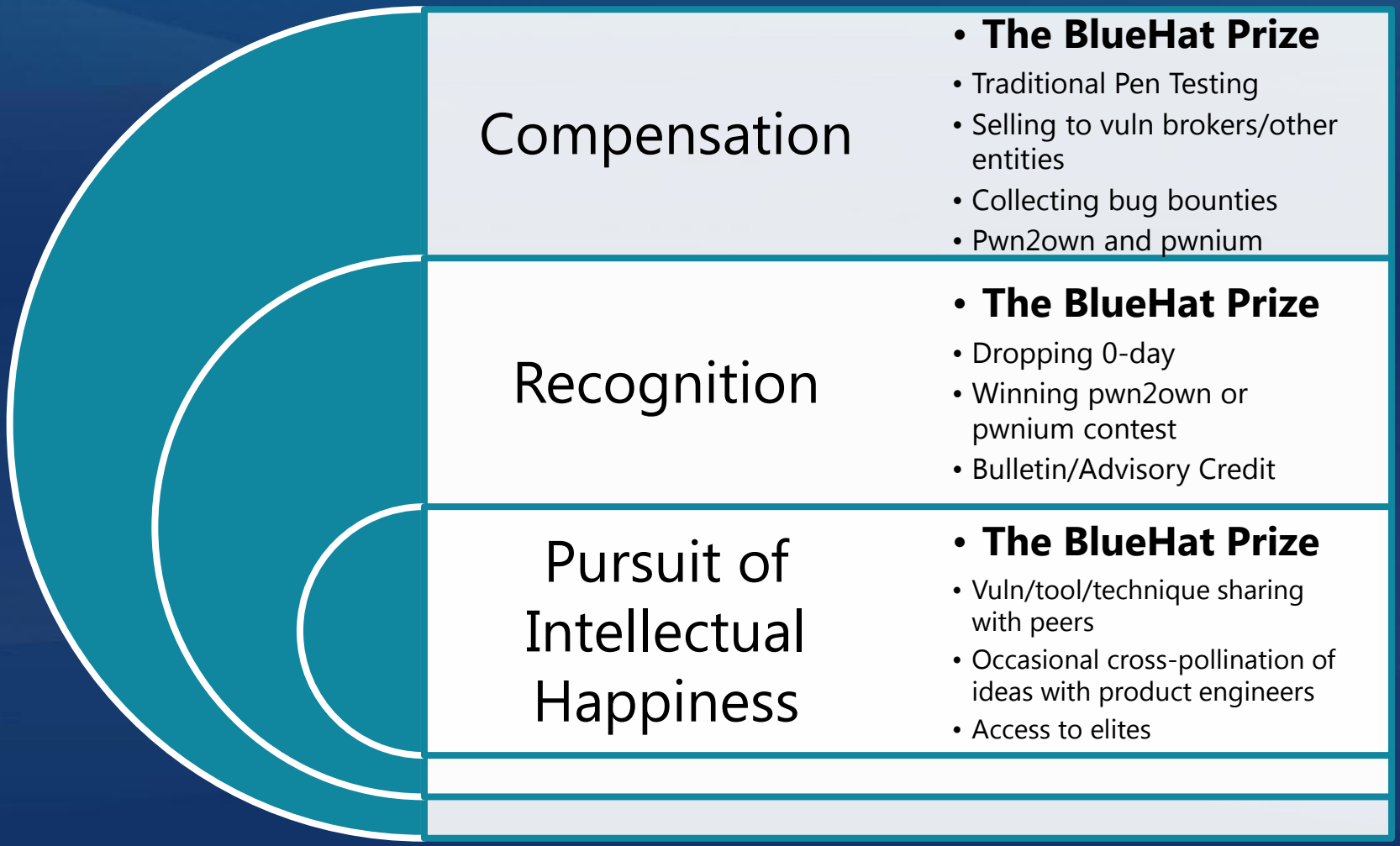
- Build mitigations that add brittleness to exploits
- Make exploits impossible to write completely reliably

Decrease opportunity to recover investment

- Shrink window of vulnerability
- Fewer opportunities via artificial diversity
- Work on rapid detection & suppression of exploit usage

$$Attacker\ ROI = \frac{\left(\frac{Gain}{Opportunity} \times N\ Opportunities\right) - (Vulnerability\ Cost + Exploitation\ Cost)}{(Vulnerability\ Cost + Exploitation\ Cost)}$$

New Researcher Motivations/Fulfillment



So What About Vendors?

Cliques at ISO High

- Subject Matter Experts (SMEs)
  - Real world/technical experience
  - May not have ISO experience
- ISO experts
  - ISO process experts
  - Most mean well
  - Subject Matter Expertise not required

(Nerds)

(Jocks)

A Tale of Two Standards

- ISO Standard of Vulnerability Disclosure (29147)
  - Dictates how vendors should deal with vulnerability reports from external finders
- ISO Standard on Vulnerability Handling Processes (30111)
  - Dictates how vendors should investigate, triage, and resolve ALL potential vulns, whether reported from external finders, or via the vendor's internal testing

Vulnerability Disclosure Standard

- Vendors should have a clear way to receive vuln reports
- Vendors should acknowledge receipt of vuln reports within one week
- Vendors should coordinate with finders
- Vendors should issue advisories that contain useful information
  - Affected products
  - Impact/severity if vuln is exploited
  - How to protect yourself

Vulnerability Handling Standard

- Vendors should have a process and organizational structure to support vuln investigation and remediation
- Vendors should perform root cause analysis
- Vendors should weigh various remediation options to adjust for real world risk factors
  - Balance speed with thoroughness
- Vendors should try to coordinate with other vendors if appropriate (multi-vendor issues)

How ISO Will Affect Your Life

- Vuln Disclosure Standard (29147)
  - Help make it easier for finders to report vulns to vendors
  - Help make the advisories a vendor releases more useful
- Vuln Handling Standard (30111)
  - Help raise the level of security investigation and remediation that vendors do

Conclusion

- Vulnerability Disclosure Need Not Be (as) Painful (for you or the vendor)
- Coordinate coordinate coordinate
- For Online Services Vuln Reporting
  - Check the laws in your country
  - Check the policy of your intended research target
  - Know the magical intersection of the above, or get permission
- For some legit $$
  - Pen test (building strong relationships with vendors helps)
  - White Market brokers
  - Vendor Bounties
  - Exploit Contests
  - BlueHat Prize for security defense
- ISO Standards in 2013
  - Vulnerability Disclosure (29147)
  - Vulnerability Handling Processes (30111)

For More Information…

- BlueHat Prize Web site: www.bluehatprize.com
- MSRC Blog: http://blogs.technet.com/msrc
- EcoStrat Blog: http://blogs.technet.com/ecostrat/
- SRD Blog: http://blogs.technet.com/srd
- Help Defend the Planet: http://careers.microsoft.com
- Follow us on Twitter:

Microsoft®

Your potential. Our passion.™