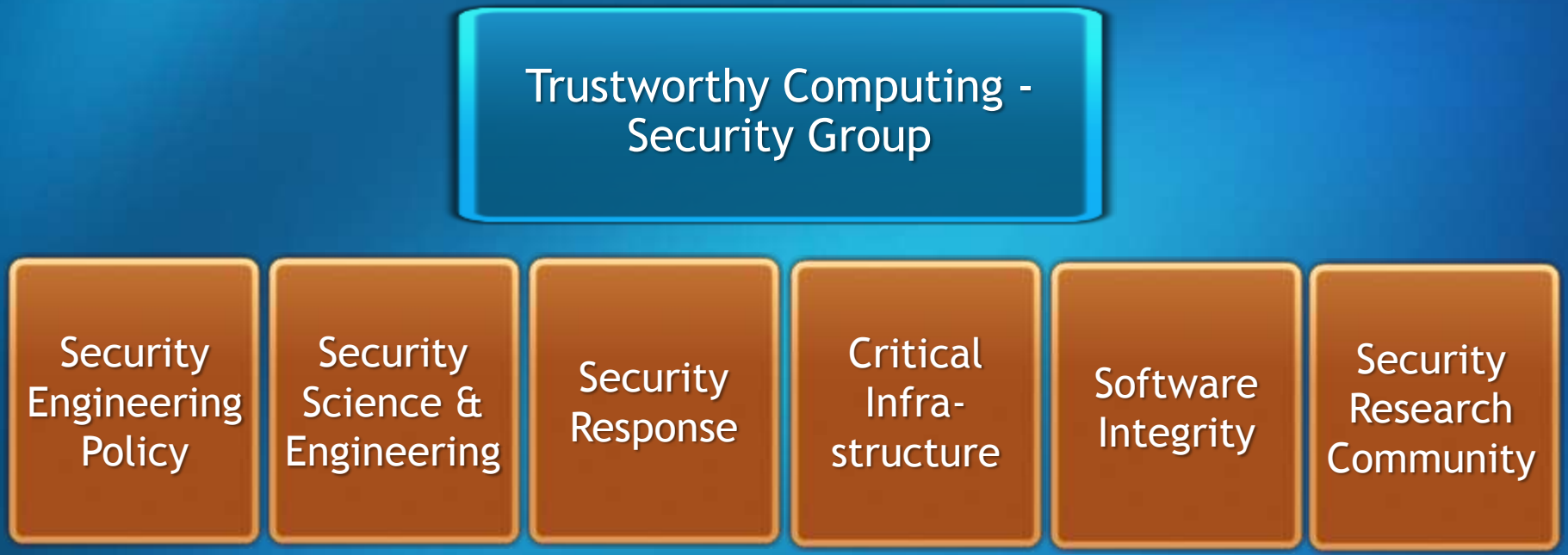
# Strategies for Evolving Threats

Andrew Cushman
Senior Director
Trustworthy Computing Security
Microsoft Corporation

# Intro – Who Am I ?

- Joined Microsoft in 1990
- Worked on MSMoney, IIS, and now Security
- Also Worked on “Patch Tuesday” & BlueHat
- Now Focused on Ecosystem Change
  - End to End Trust & Collective Defense



# Intro – Why Am I Here?

- Brasil is Special & Unique
  - Geography, People, Culture, Economy, Security
- Microsoft & Andrew are committed Brasil
  - Share Expertise & Help Build Capability
- Brazilian Opportunities (& Challenges)
- Discuss Framework & Strategies
  - Cyber Threat Maturity Models
  - Cyber Threat (Lifecycle) Management
  - Collective Defense
- Listen & Learn & Ask for Suggestions

# Usual Impressions of Brazil

- Samba & Carnaval
- Bossa Nova
- Soccer
- Beaches & bathing suits
- Favelas

- Churrascaria
- Online Banking usage
- Cyber Crime

# Things most people don't know...

- 7th largest IT market WW
- 6th country in PC Shipments WW
- **3rd in online time** per user – 22h50min/month
- **5th largest cell phone market** - 147M units
- **60% of all 3G Cell Phones in Latin America**
- **2nd largest WW in number of Companies** (620k new Companies only in 2010)
- In the last 5 years, **internet active users in total Population grew from 24% to 43%** in 2009
- **10th in broadband (256 kb) users** - 9.1M users (4.8% of total 190M population)

# Why Andrew Loves Brasil

- People –
  - Friendly, Smart, Hard
    Stylish!, Proud & Hur
- Culture
  - Diverse Society and a
  - Di Cavalcanti, Viniciu
- Land of Opportunity
  - Geography – Huge co
    resources (and peopl
  - Government - Found
    Law
- It Works
  - There is a Brazilian Way

# Andrew's Goals in Brasil

- Help reduce the cyber threat environment
  - Collective Defense to Reduce threats (MAPP& DISP)
  - Build government capacity (CERT outreach, CIPP),
  - Partner w/ Enterprises
- Be a Trusted Advisor
  - Help Reduce the Policy Complexity
  - Best practices – technical, policy, and procedures
- Foster awareness of MS security excellence
  - Security Engineering, Security Response
- Positively influence local innovation programs
  - Help Secure local software (SDL & other programs)

# Security Challenges in Brasil

Rapid Evolution and Adoption of Technology

# Cyber Landscape Changes

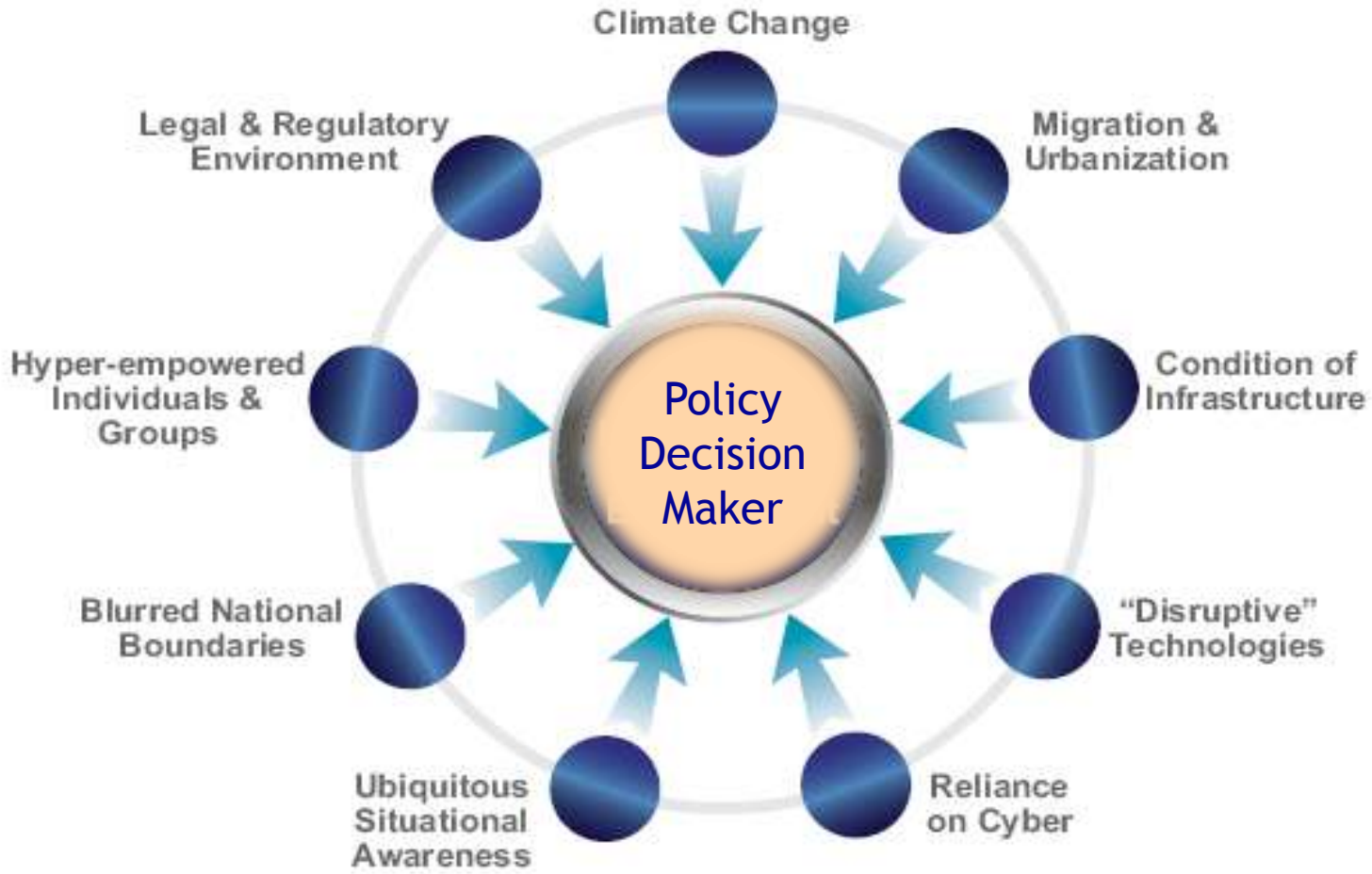
- Users:
  - More Users
  - Faster Connections
  - Average Security Awareness Score ->

- Threats:
  - Worldwide increase in volume & frequency
  - Similar pattern in Brasil
- Defense:
  - More Interaction btw the good guys
  - New tactics
  - But…

# Security Protection Complexity

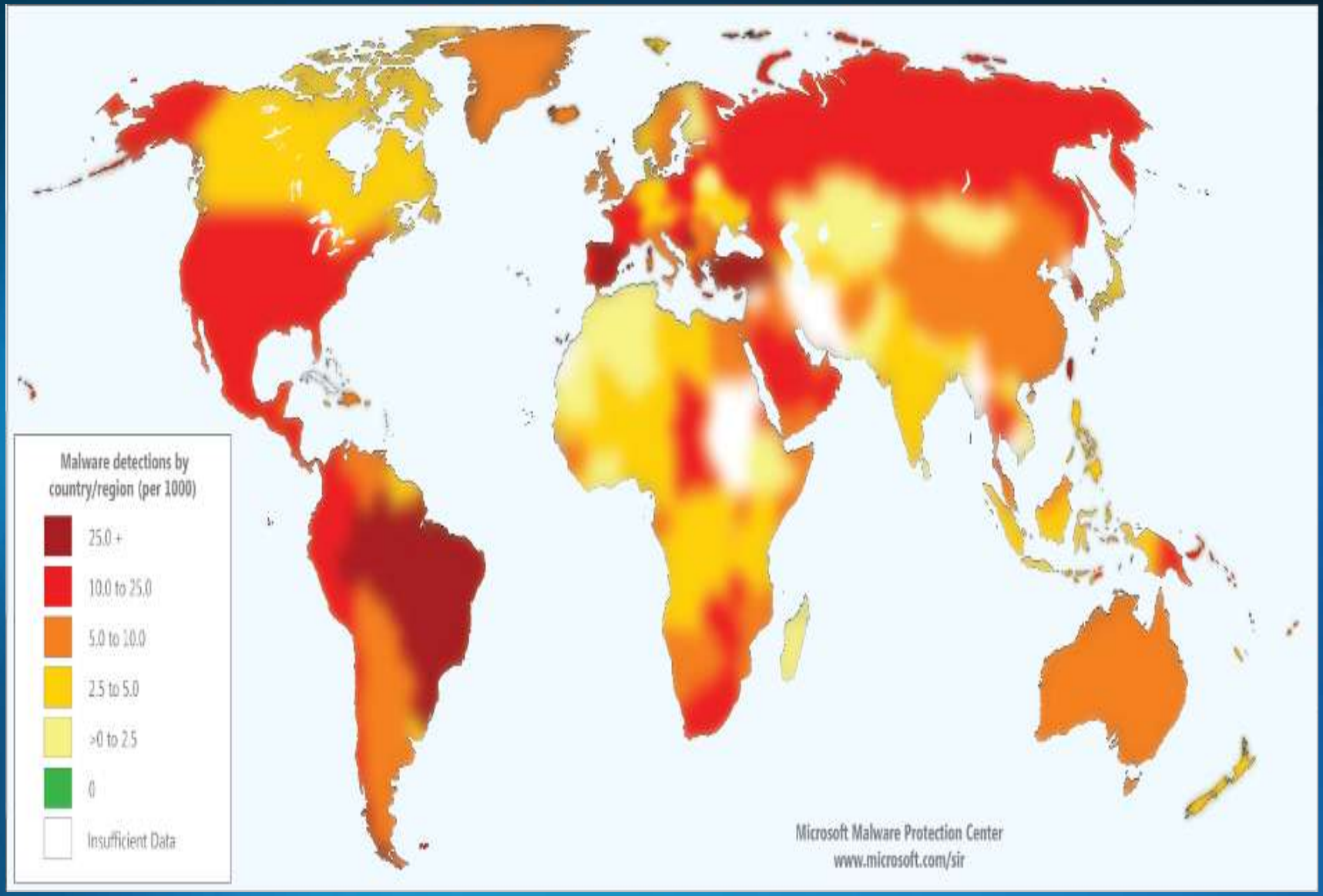

Source: modified from *Guarding Our Future Protecting Our Nation 's Infrastructure*
Toffler Associates 2008

# Security Policy Complexity

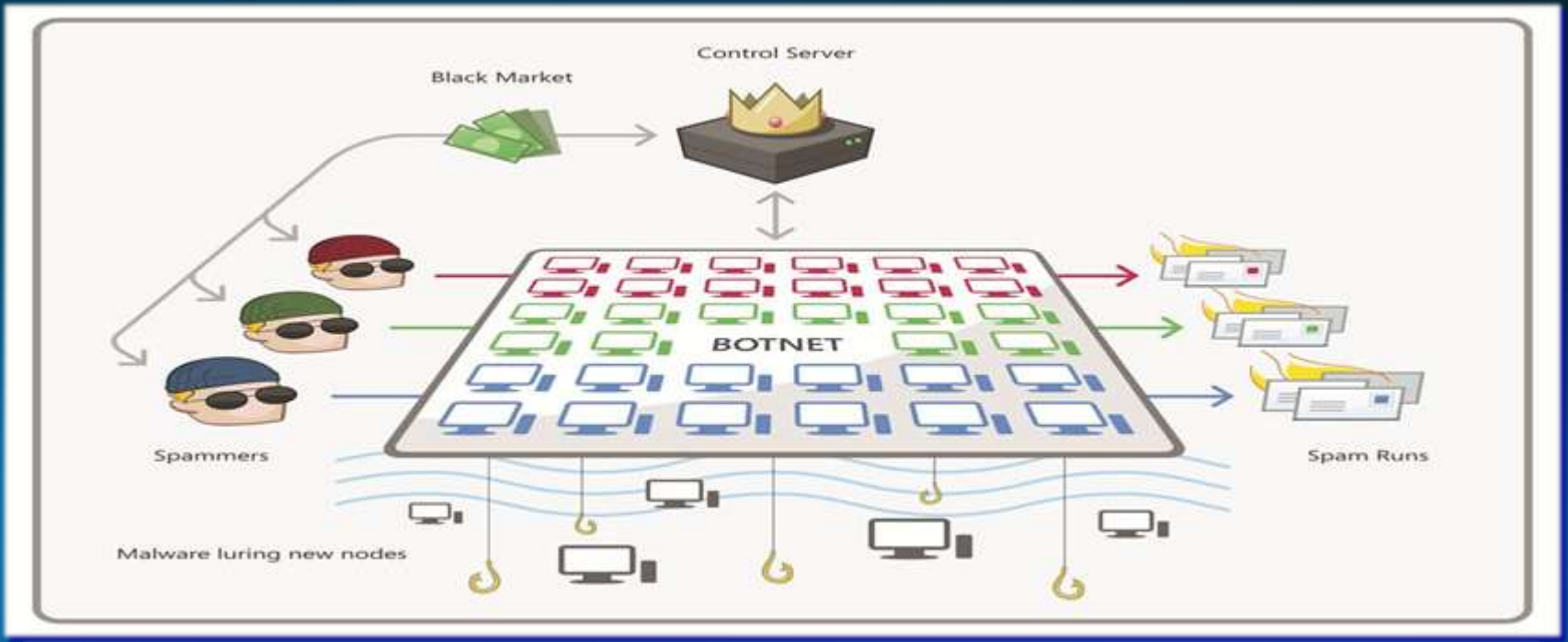



Source: modified from *Guarding Our Future Protecting Our Nation 's Infrastructure*
Toffler Associates 2008

# SIR v9 World-wide Infections



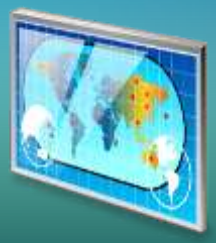
# Same Tactics – Different Targets & Controllers




Cybercrime

Military Espionage

Economic Espionage



Cyber Warfare

# Security Maturity & Lifecycle Frameworks

# Cyber Security Maturity Model

# Threat Lifecycle Management (simplified)

## Protect

Asset Classification
Identity Mgmt
- Users
- Devices

Access Control
- Network
- Machine & Data

Training

## Recover

Update
- Software
- Hardware
- Procedures
- Training
- Defenses

Restore
- Data & Facilities


## Detect

Monitor
- Baseline
- Intrusions

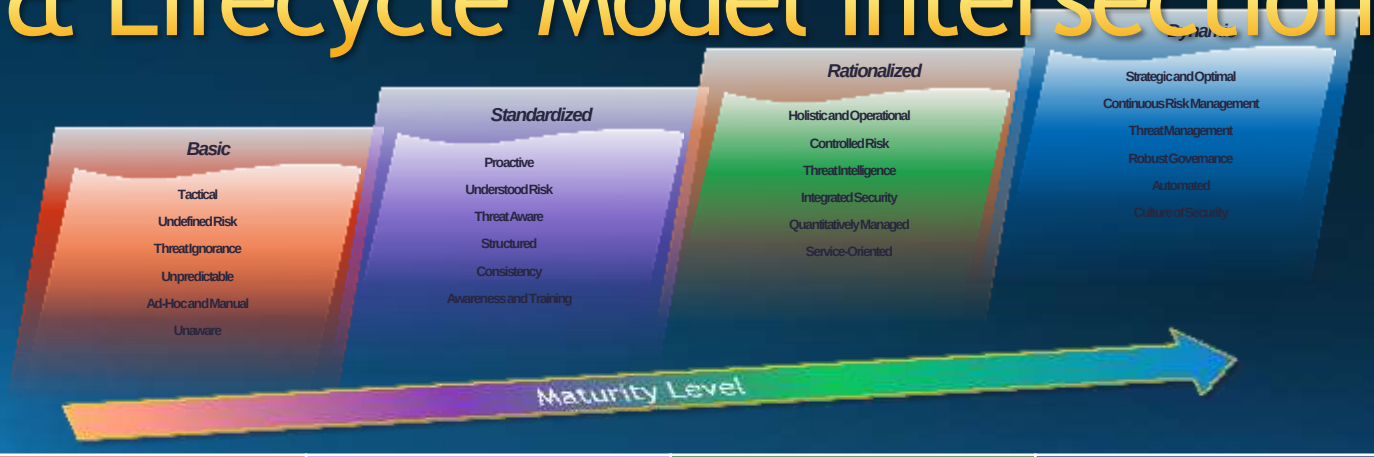
Assessment
- Vulnerabilities
- Configurations

Reporting

## Respond

Incident Response
Emergency response
Communicate
Remediate
- Quarantine
- Clean
- Patch

# Maturity & Lifecycle Model Intersection


| | Basic | Standardized | Rationalized | Dynamic |
|---|---|---|---|---|
| Protect | - Desktop Image Engineering<br>- Active Directory Design & Deployment<br>- BitLocker Full-Volume Encryption | - Desktop Optimization and Configuration Management<br>- Security for Wireless Services<br>- Secure Public Key Infrastructure Solutions<br>- Strong Authentication using Smartcards<br>- Application Lifecycle Management Services 2010<br>- Network Access Protection with 802.1x Enforcement | - Desktop Virtualization Solutions<br>- Server Virtualization with Advanced Management - Virtual Desktop Infrastructure<br>- Network Access Protection with IPSec Enforcement<br>- Network Isolation Services<br>- Secure Web & Remote Access using Forefront TMG<br>- Enterprise Identity Lifecycle Management<br>- Data Protection using Active Directory Rights Management | - Server Virtualization with Advanced Management - High Availability Solution<br>- Seamless Access using DirectAccess and TMG<br>- Enterprise Federated Identity using ADFS<br>- Application Backup using System Center Data Protection Manager |
| Detect | - Client Anti-Malware Solutions | - Enterprise Configuration Management<br>- IT Enterprise Management: End-to-End Cross-Platform Monitoring<br>- Enterprise Mobile Device Management<br>- Client and Server Anti-Malware Solutions<br>- Windows Error Reporting Deployment Services | - IT Compliance and Reporting: End-to-End Monitoring<br>- Audit Collection Services<br>- System Error Reporting & Analysis Services | - Server Virtualization with Advanced Management - Centralized, Policy-driven Management |
| Respond | - Premier IR Support and Training | - Secure Development Lifecycle Training and Assessment Services<br>- Internet Crime and Forensics Investigations Education and Training Services | | |
| Recover | - Enterprise Recovery Services | | | |

# Collective Defense Framework

# Collective Defense

- We need new ideas mechanisms to manage today's threats
- Need better preventative measures and
- Need better response mechanisms
- Public health ideas have been proposed
- ISP Anti-Botnet (Walled Garden / Quarantine) solutions are being deployed

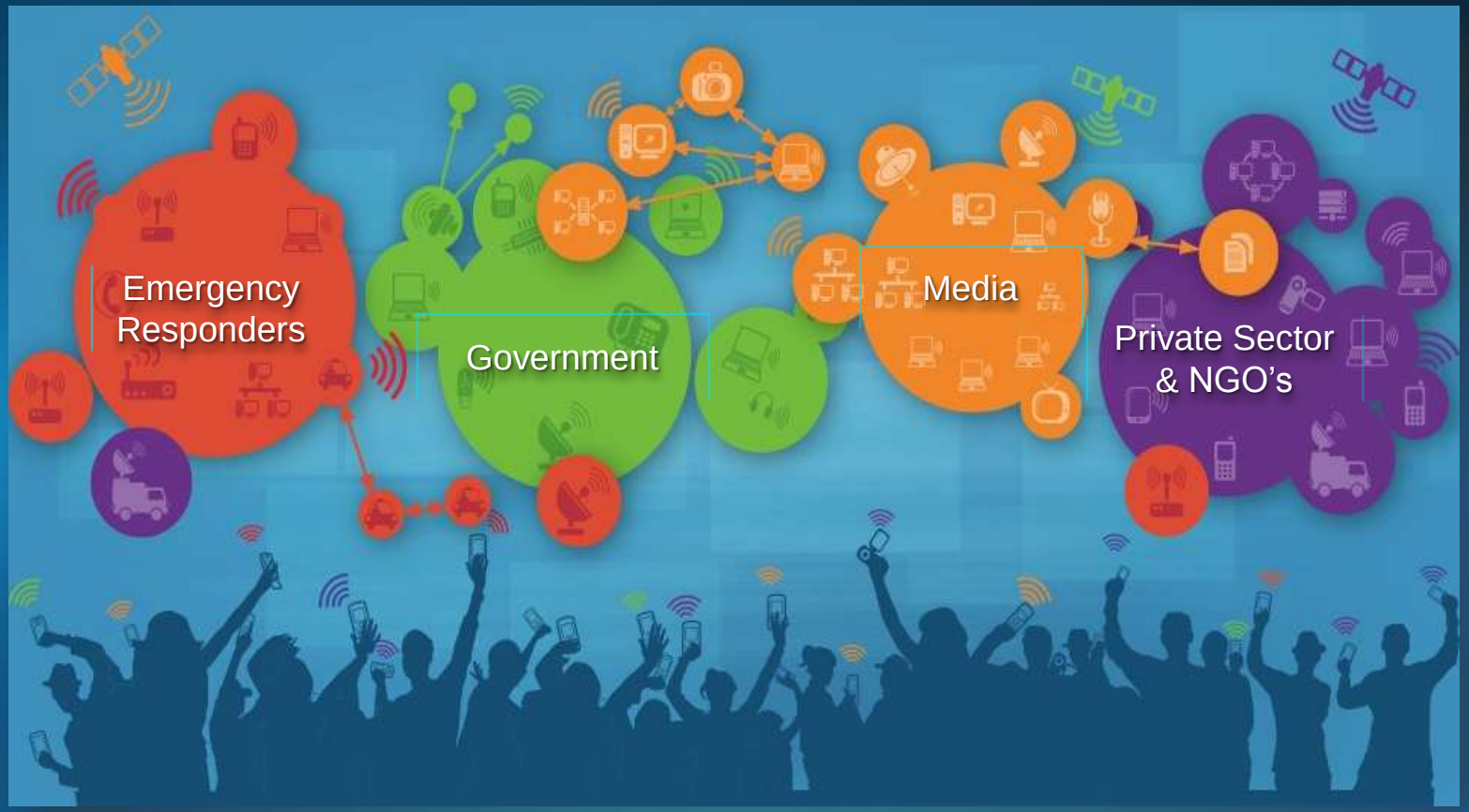
# Problem Dimensions

- Population (users and devices):
  - Need awareness of risks and how to manage them
  - Need to manage basic hygiene on devices
  - Vendors to provide easy to understand & use solutions
- Interactions:
  - Greater transparency needed online
  - What is the health of device? Application? Service?
- Environment:
  - “Safe Network Neighborhoods”
  - Active management of networks & devices

# Framework to Address Cyber Threats

| | Citizens | Enterprises | Government |
|---|---|---|---|
| **Population** (Users) | • Training<br>• Public Service Campaign | • Training<br>• Public Service Campaign | • Judicial Training |
| **Interactions** (Transactions) | • Machine Health Claim | • EV SSL Certs<br>• 2 factor Auth<br>• DNSSec | • Telco / ISP Regulation<br>• e-ID |
| **Environment** (Network) | • e-ID | • Quarantine | • Botnet Takedown |

# Collective Defense – Participants




Many Diverse Participants in Cyber Incidents
Collective Defense means aligning efforts to maximize effectiveness and minimize unintended consequences

# Challenges Ahead…

Things that give me pause…

# Andrew's Worry List…

- Growing Online Transactions
  - Online Banking has been secured – what about other online transactions / social interactions?
- Uneven Growth
  - Can security keep up with innovation?
    - Awareness / engineering / response
  - Will the "weakest links" be strong enough in 2014 & 2016?
- RIC – national eID
  - Balance privacy and security and usage
  - What can be learned from Germany and Austria?
- Expanded Broadband Access
  - Giving the bad guys fat pipes ?
  - Is a Walled Garden possible in Brasil

# How can I help in Brasil?

Some future investment areas where I might help

- Counter eCrime & Malware
- RIC - National Digital ID
- ISP (& Broadband) Project
- Critical Infrastructure Protection Programs
- New Cyber Defense Center(?)
- BlueHat SP - Connecting Segments
- Security Engineering & Secure Development Lifecycle

- Other?

# Questions:

- Is my “worry list” too long?
- Is it incomplete?

- Are the Future Activities & Investments unnecessary?

# Resources

Microsoft Security Intelligence Report

- http://www.microsoft.com/SIR
- http://www.microsoft.com/security/sir/threat/default.aspx#brazil

Collective Defense Whitepaper – Scott Charney

- http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/internethealth.aspx

ISP Anti-Botnet Activities

Cyber Clean Center (English Report)

- https://www.ccc.go.jp/en_report/Report_on_the_activities_of_the_Cyber_Clean_Center.pdf

Comcast – USA -

- http://news.cnet.com/8301-27080_3-20018168-245.html?part=rss&subj=news&tag=2547-1_3-0-20

Australia

- http://iia.net.au/images/resources/pdf/icode-v1.pdf

Germany

- http://www.oecd.org/dataoecd/42/50/45509383.pdf

Microsoft®

Your potential. Our passion.™