

Recent Cybersecurity Development and Implications

Meng-Chow Kang, PhD, CISSP, CISA
Director and CISO

Asia Pacific, Japan, and Greater China, Cisco Systems

Mobility

Cloud

Social
networking

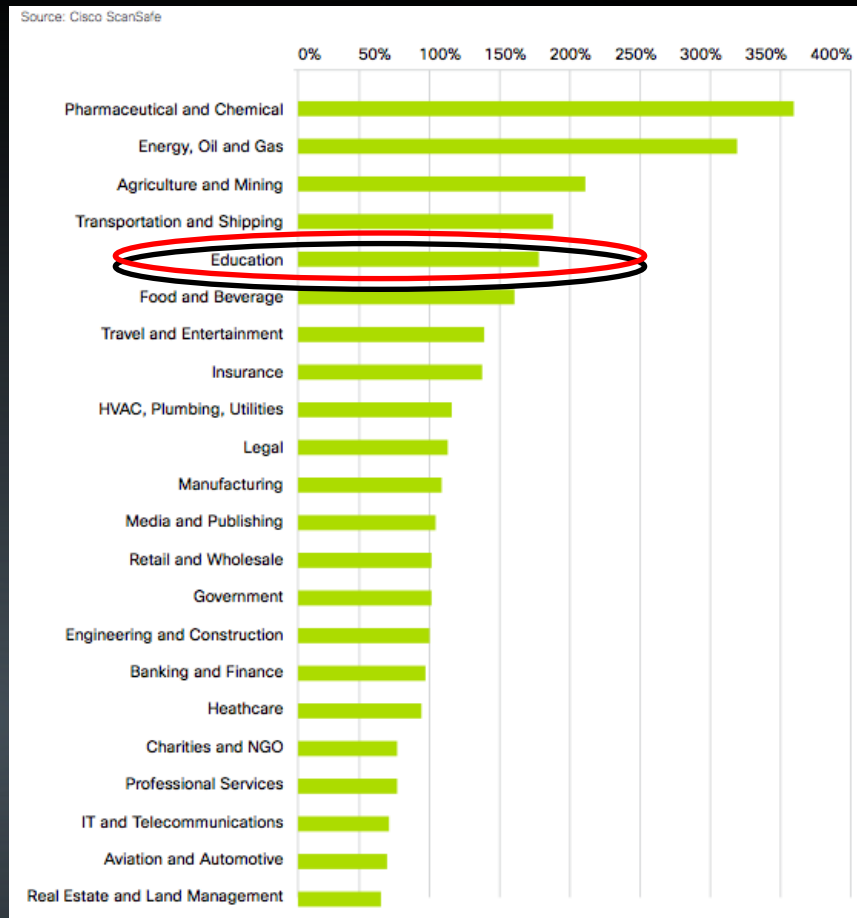
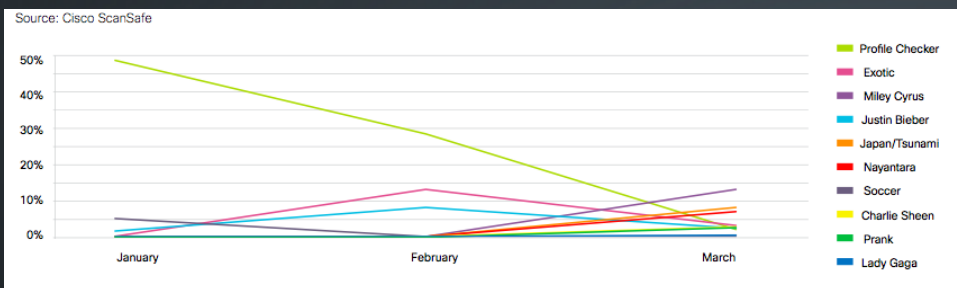
Personal Devices

Consumerization of IT



Cisco Q1 FY11 Global Threat Report

- Enterprise users experienced an average of 274 Web malware encounters per month in 1Q11, a 103% increase compared to 2010.
- “Likejacking” encounters increased significantly during 1Q11, from 0.54% of all Web malware in January 2011 to 6% in March 2011.

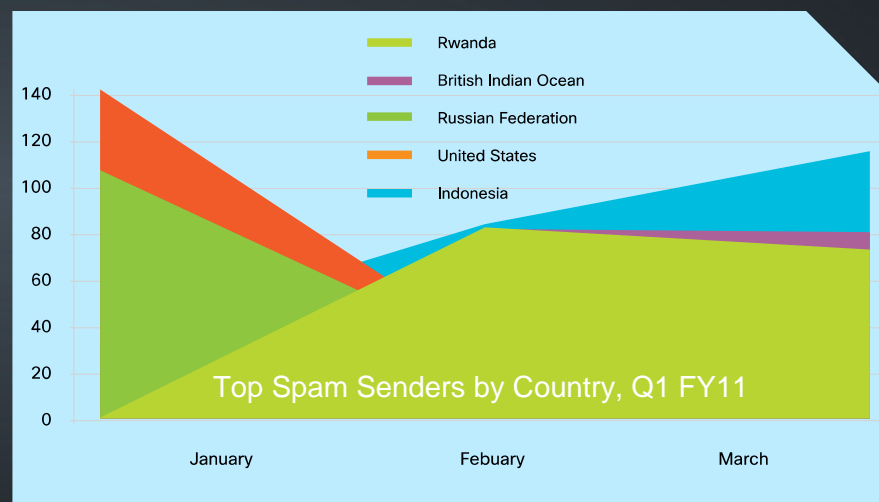


Cisco Q1 FY11 Global Threat Report (cont.)

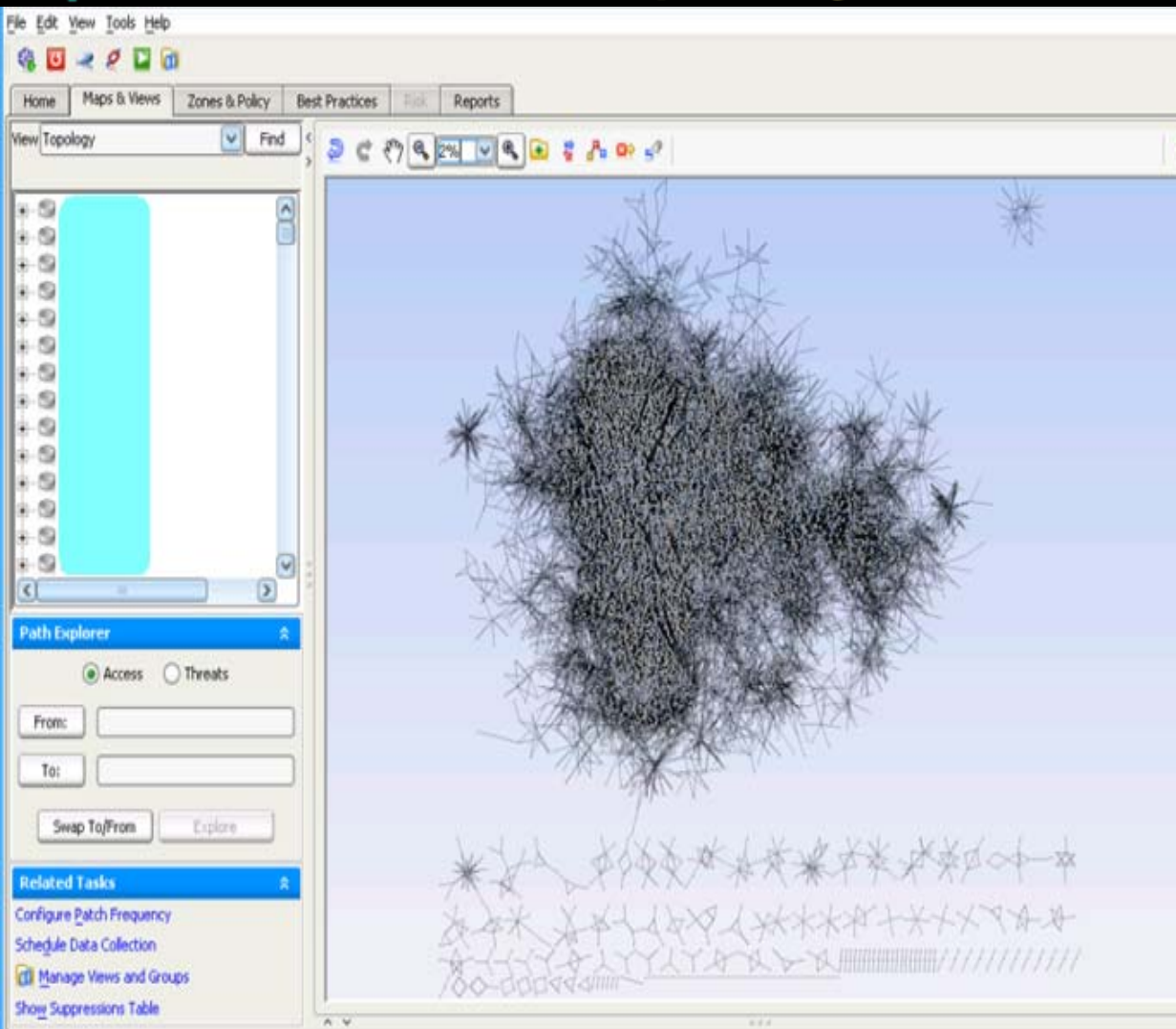
Attacks on cloud services, and social networks are prevalent

- Denial-of-Service (DoS) attacks are increasingly politically and financially motivated.
- In 1Q11, attackers increasingly turned their attention toward phishing Twitter accounts
- The 2011 takedown of segments of Rustock, combined with multiple spam botnet takedowns in 2010, had a positive impact on overall spam volume. However, spam volume in 1Q11 remained above the lowest point recorded in December 2010.

Signature	Events
Generic SQL Injection	55.03%
Web View Script Injection Vulnerability	7.01%
Gbot Command and Control Over HTTP	5.16%
B02K-UDP	5.20%
Cisco Unified Videoconferencing Remote Command Injection	4.91%
Microsoft Internet Explorer Invalid Flag Reference Remote Code Execution	3.27%
Windows MHTML Protocol Handler Script Execution	2.47%
WWW WinNT cmd.exe Access	1.30%
Web Application Security Test/Attack	1.19%
MyDoom Virus Activity	1.16%



Technology & Users are not the main problem... Complexity Is



IPv6

- 3ffe:1900:4545:3:200:f8ff:fe21:67cf or
- fe80:0:0:0:200:f8ff:fe21:67cf or
- fe80::200:f8ff:fe21:67cf

Tunneling

- Router-to-router
- Router-to-host
- Host-to-route
- Host-to-host
- Multi-homing

Mobile Ad-Hoc Networks

- Mesh
- Wireless
- Vehicle MANET
- Intelligent vehicle MANET
- Internet-based MANET

Miniaturization

Multi-Purpose Devices

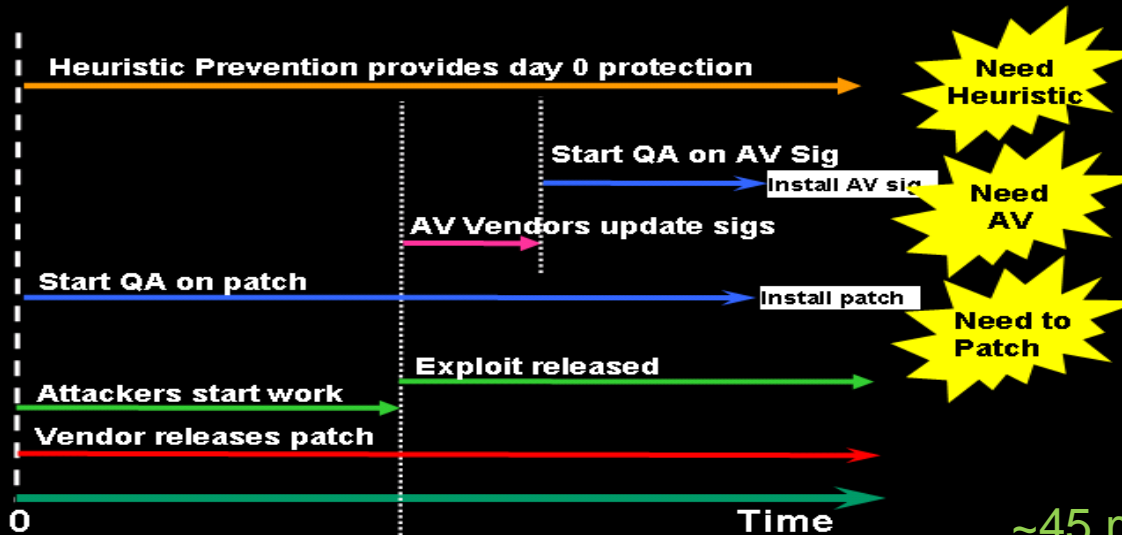
Eradication of Perimeters

- Partners, customers, government, competitors, public

Virtualization

Cloud Computing

Traditional Practice is Losing Effectiveness

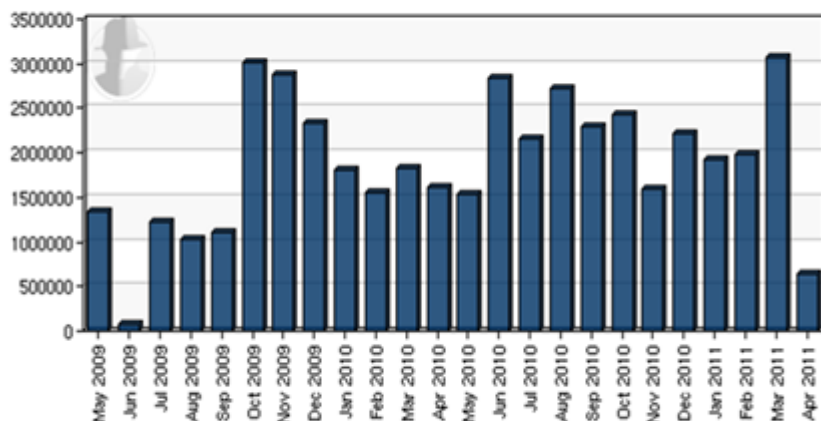


www.shadowserver.org/

14 April 2011

~45 million new hashed binaries in the past year; ~92 million total seen

New Samples



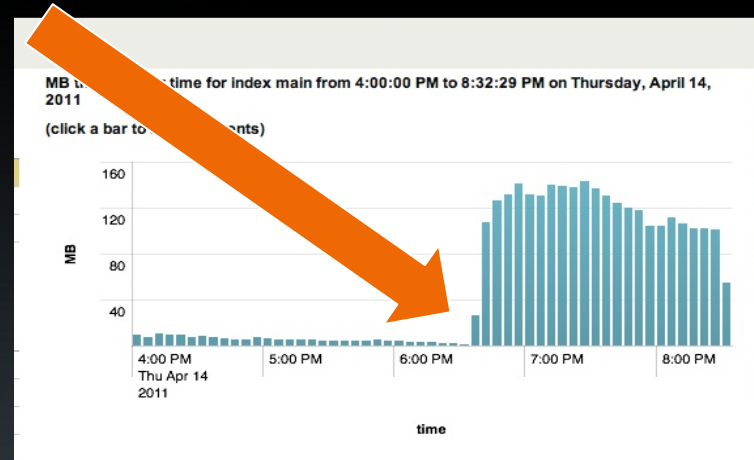
Binary Count



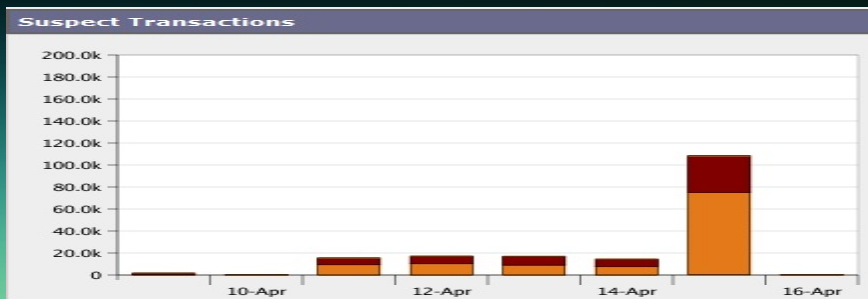
Web Security – Global Deployment

Malicious Transactions Blocked

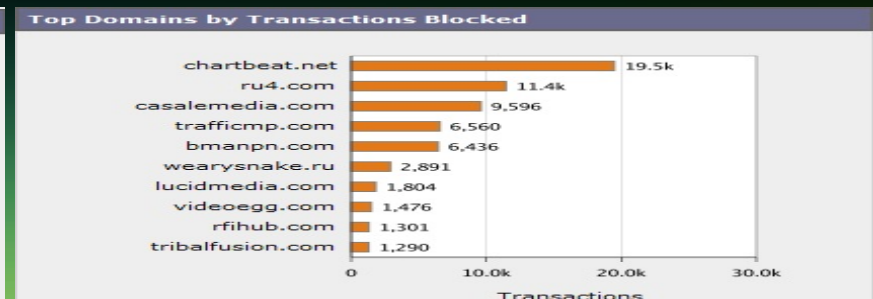
- From pilot (rtp campus) to global (phase 1)
- Total Blocked within **4 hours**: 65,000 including:
 - Malware downloads
 - Browser hijacking software
 - Unwanted advertisement software
 - Botnet check-ins
 - Trojan (backdoor) connections



- Average response to client: **1.4 seconds** (*no change from pilot*)
- Average daily log data: **25+ Gb** (*more than double from pilot*)
- *No System Resource Utilization (CPU, RAM) impact*



Suspect Transactions



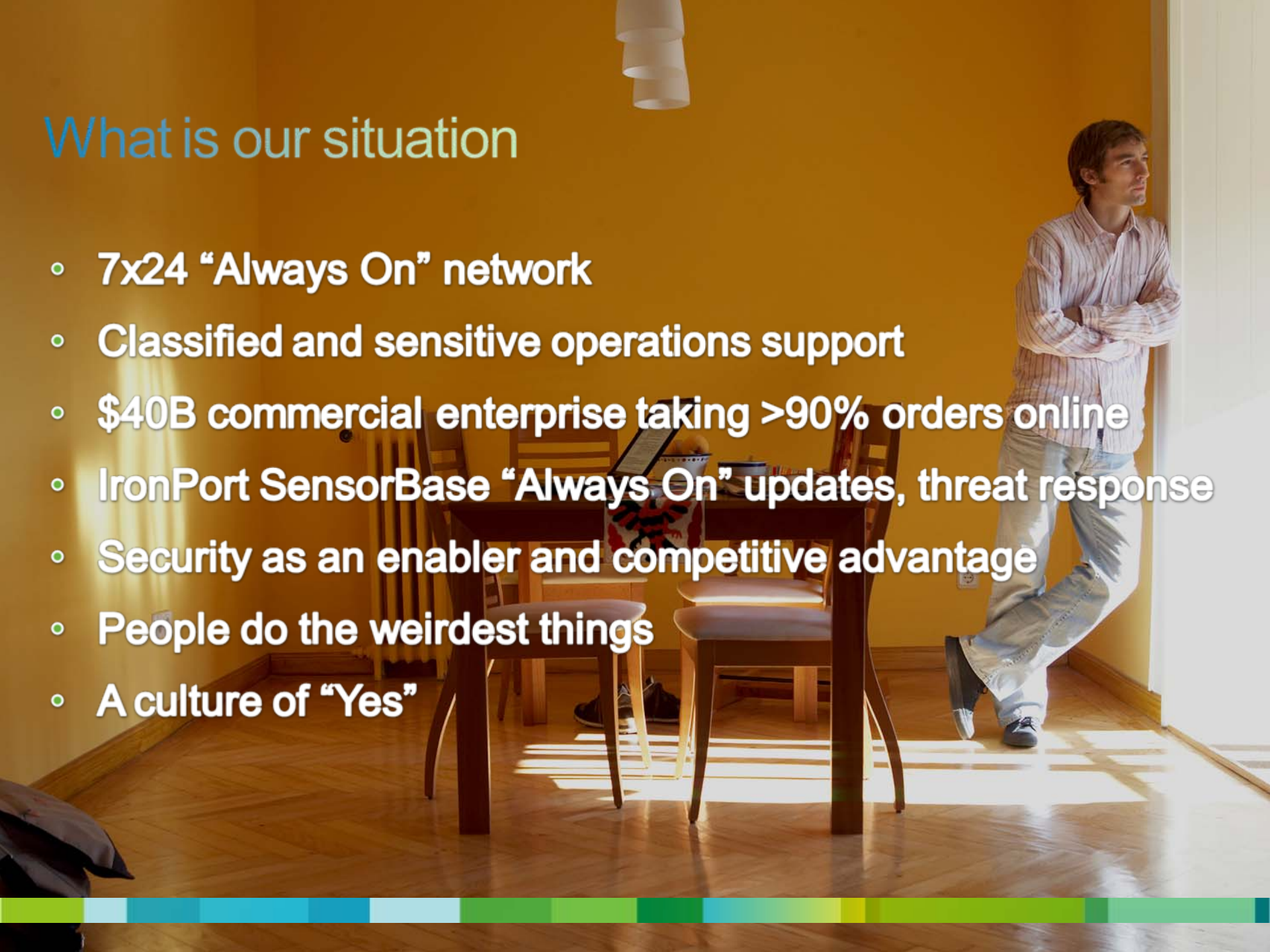
Top 10 Blocked Domains

Security Objectives

- Keep the bad stuff out of your environment
- Keep the good stuff in and protected
- Keep critical services up and running
- See what I need to see
- Enable productivity through choice and secure connectivity
- Be “In bounds” (compliant, provable, policy, legal, etc.)

What is our situation

- 7x24 “Always On” network
- Classified and sensitive operations support
- \$40B commercial enterprise taking >90% orders online
- IronPort SensorBase “Always On” updates, threat response
- Security as an enabler and competitive advantage
- People do the weirdest things
- A culture of “Yes”



Global Flow of Information

1010101010101010
0101010101010101
1010101010101010
0101010101010101
1010101010101010
0101010101010101

[illegible][illegible]

5 Exabytes per month

1.4 Billion DVDs crossing the network

2007

21 Exabytes per month

4.8 Billion DVDs crossing the network

2010

56 Exabytes per month

12.8 Billion DVDs
crossing the network

2013

Growth of Connected Devices

Total 500 Million **Total** 12.5 Billion **Total** 25 Billion **Total** 50 Billion



$\frac{1}{8}^{\text{th}}$ Connected Device
per Person worldwide

2003



1.84 Connected Devices
per Person worldwide

2010



3.47 Connected Devices
per Person worldwide

2015



6.58 Connected Devices
per Person worldwide

2020

2008

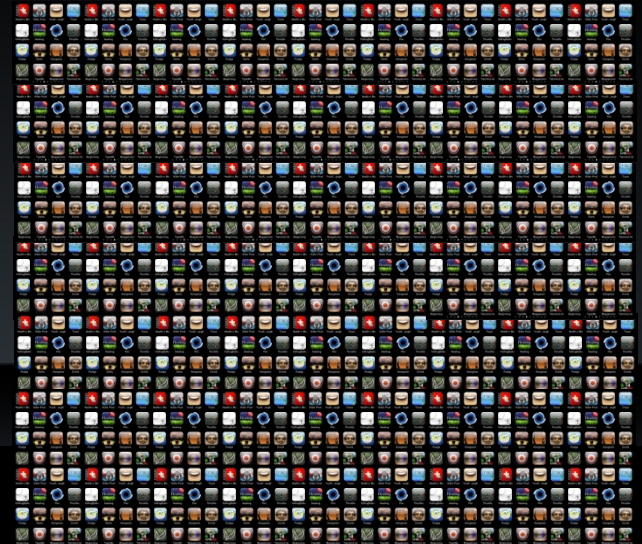


More connected devices than people

World of Applications

Total Mobile Apps **iPhone** Apps Alone

Apps Worldwide



3,000

2007

160,000

2010

350,000

2011

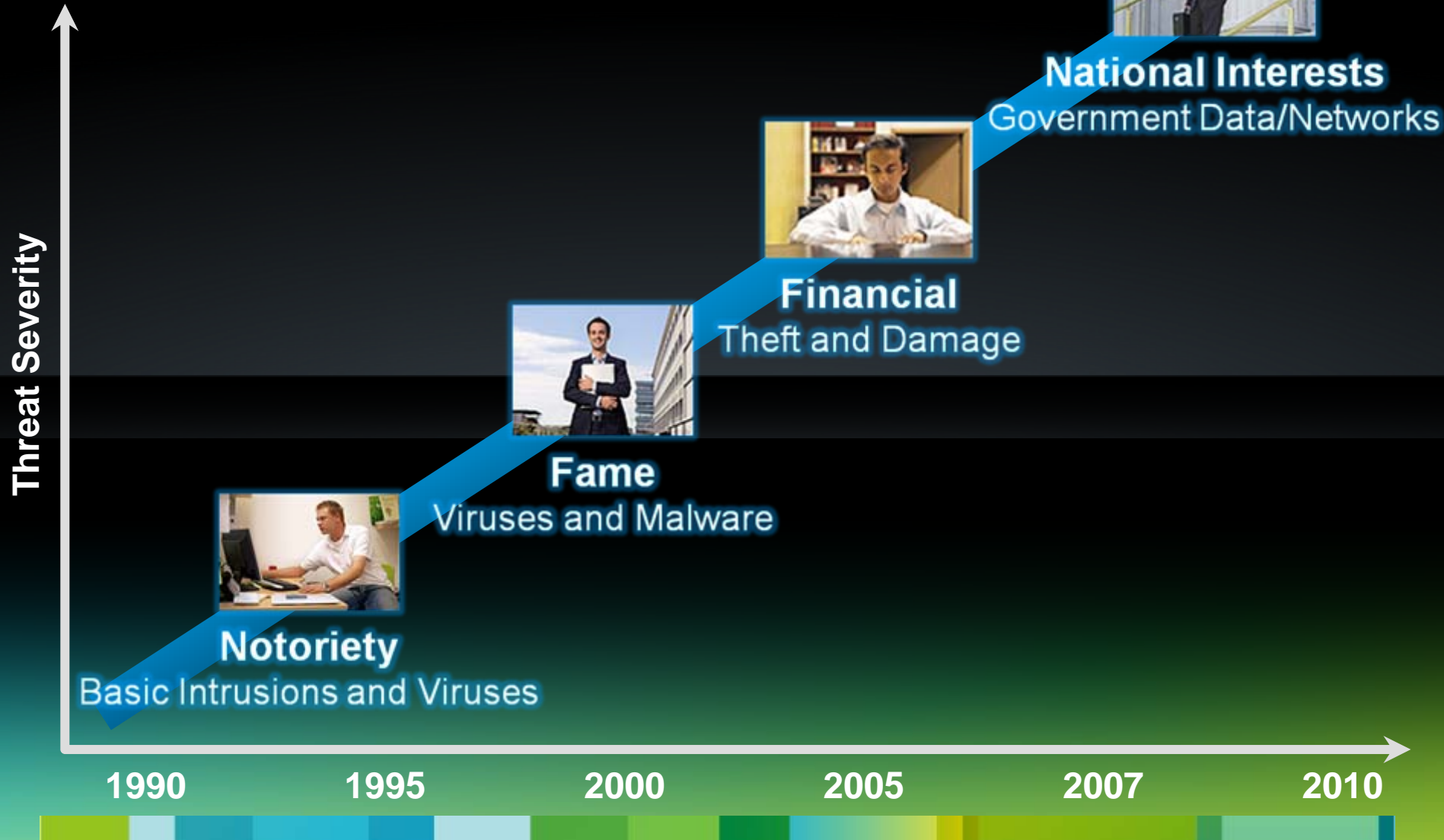
1,500,000

2013

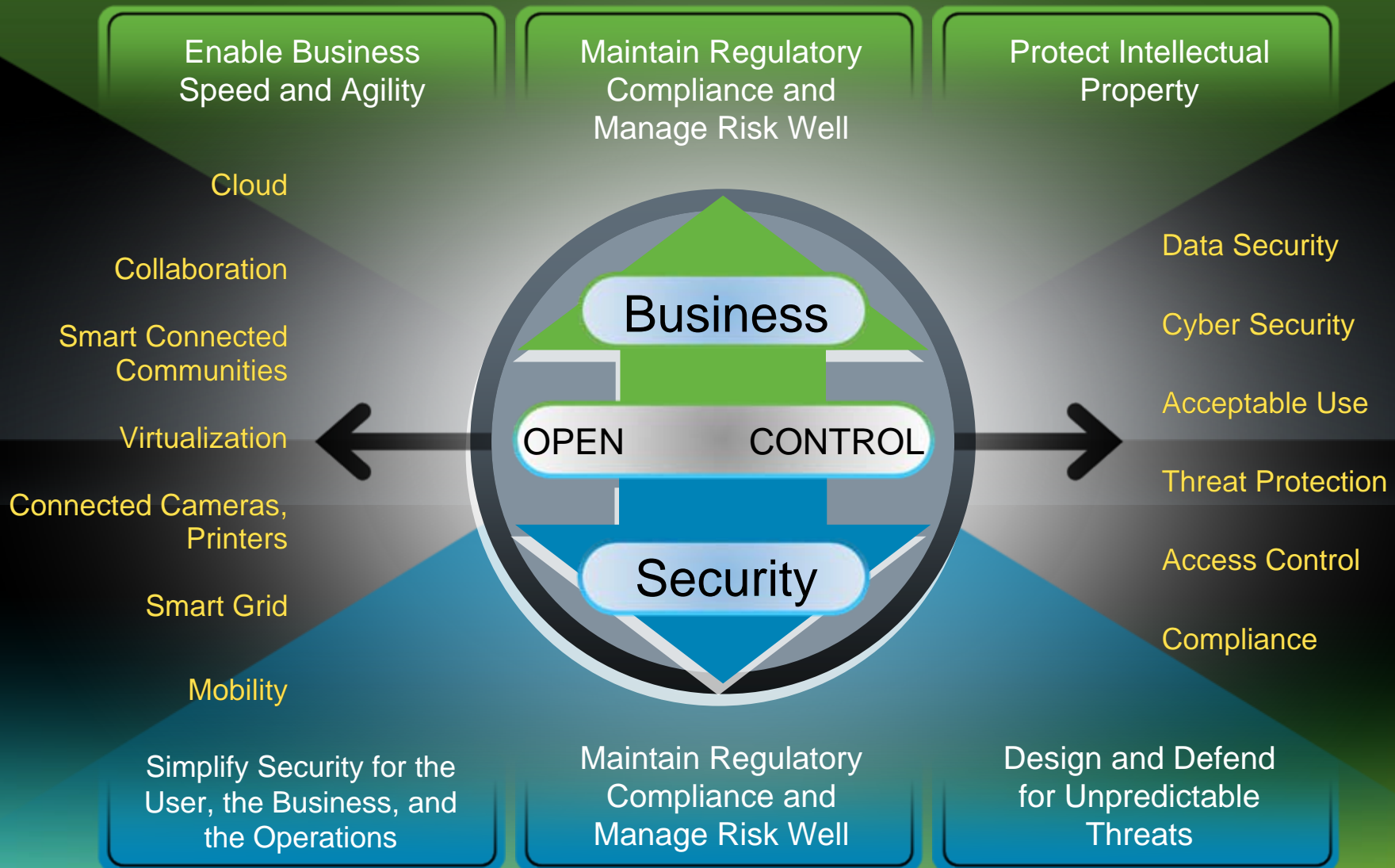


Evolution of the Threat Landscape

Increasingly Difficult to Detect and Mitigate



Harmony



Key Points

Manual

Borders

Unknown



Automated

Everywhere

Known



Ignore Headlines, Look for Trend Lines

National Journal

[HOME](#)[WHITE HOUSE](#)[POLITICS](#)[CONGRESS](#)[DOMESTIC POLICY](#)[NATIONAL SECURITY](#)

Tech Daily Dose

POLITICS & POLICY IN A WIRED WORLD

DHS Official: Cyber Attacks against Infrastructure on the Rise

By Chris Strohm

1/26

DHS Official: Cyber Attacks against Infrastructure on the Rise

See, Don't Feel – Analyze

Data Removes Emotion

Understanding /
Strategy /
Action

Hosting

Net Team

SecOps

Others

Information

Event /
Behavior
Correlation

Network Analysis

System Analysis

Security Vendor

Others

Identity

Geo
Location

Proximity

Homegrown
Apps

Data

Sensor
Logs

SCADA

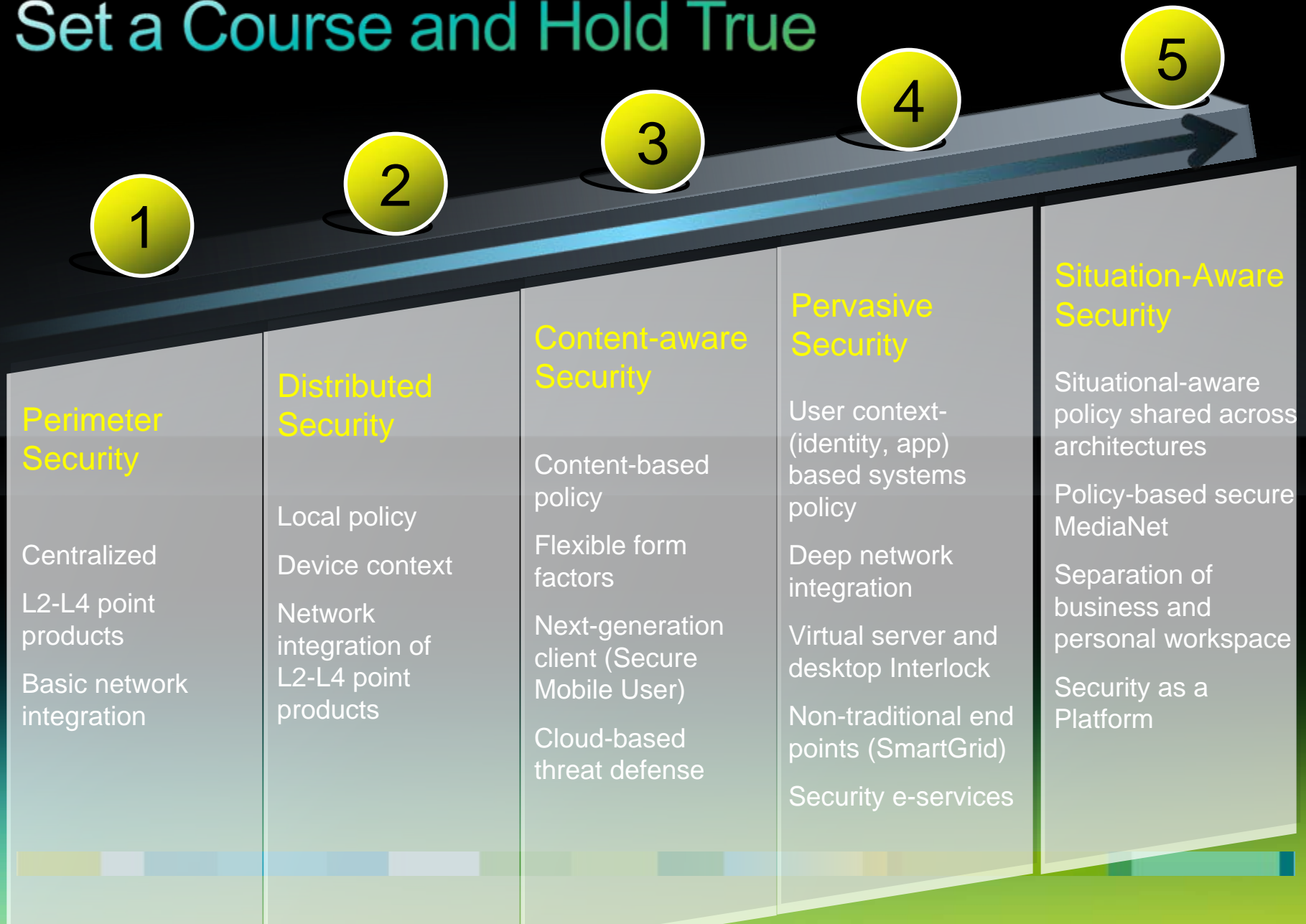
Others

“I have a series of questions, and the data gives the answers”

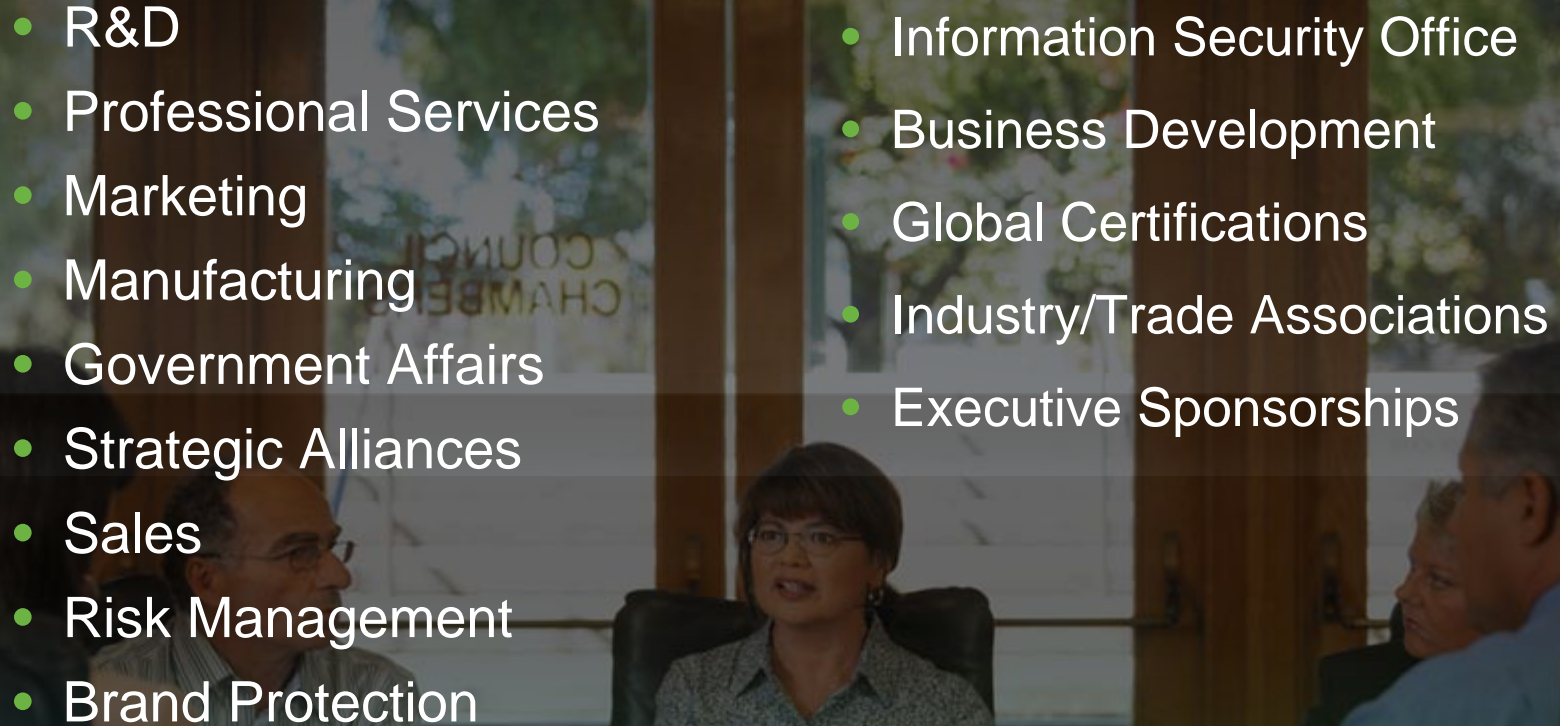
~ or ~

“I don't know the questions yet; let's look at the data”

Set a Course and Hold True



Demand Participation, Expect Accountability

- 
- R&D
 - Professional Services
 - Marketing
 - Manufacturing
 - Government Affairs
 - Strategic Alliances
 - Sales
 - Risk Management
 - Brand Protection
 - Information Security Office
 - Business Development
 - Global Certifications
 - Industry/Trade Associations
 - Executive Sponsorships

Ask The Right Questions

You get what you measure, no matter what...

Always question what you are doing – some things have declining investment and results

Stop asking for best practices – start asking “what’s effective and how effective is it?”

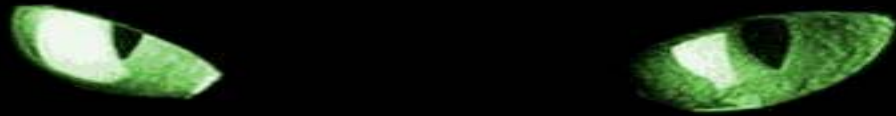
What can I see?

What don’t I know?

How will I know it when I need to?

What can I shamelessly copy from someone else?





*What is our adversary
thinking...
right...
now...
?*

Discussion/Q&A



<http://mengchow.wordpress.com/>



@mengchow

