



Lessons From Our Past Fuel The Success Of Our Future

John N. Stewart
Vice President, Chief Security Officer

14 June 2011

FIRST Conference 2011

My 3 Goals For This Session...

1. To have **you walk away considering** these ideas
2. To ensure **I don't attend another security conference** and talk about:

Private-Public Partnerships

Information Sharing

The Evolving "Threat"

3. To create **tangible action items before Malta** that we can report out on

What I've Shared to Date

2008 2000 2010 2011



*Our Role In Protecting
Critical Infrastructures*



John N. Stewart
Vice President
Chief Security Officer

First 20th Annual Conference 2008

FIRST 2008 © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

2008

2010 2011 2012 2013



Who Moved My Cheese?
Why The Security Industry
Has Been Turned
Upside Down



John N. Stewart
jns@cisco.com
Vice President
Chief Security Officer

FIRST 2010 © 2010 Cisco Systems, Inc. All rights reserved. Cisco Public

2010

FIRST Conference 2011



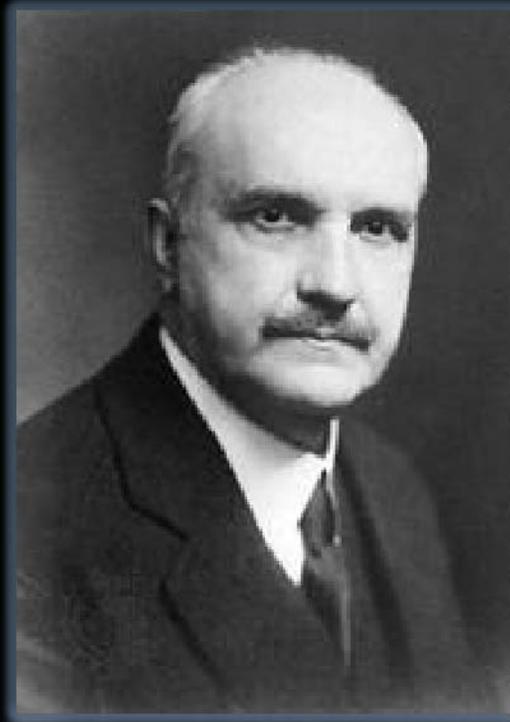
**Lessons from Our Past
Fuel the Success of Our Future**



John N. Stewart
Vice President, Chief Security Officer
14 June 2011

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public

2011

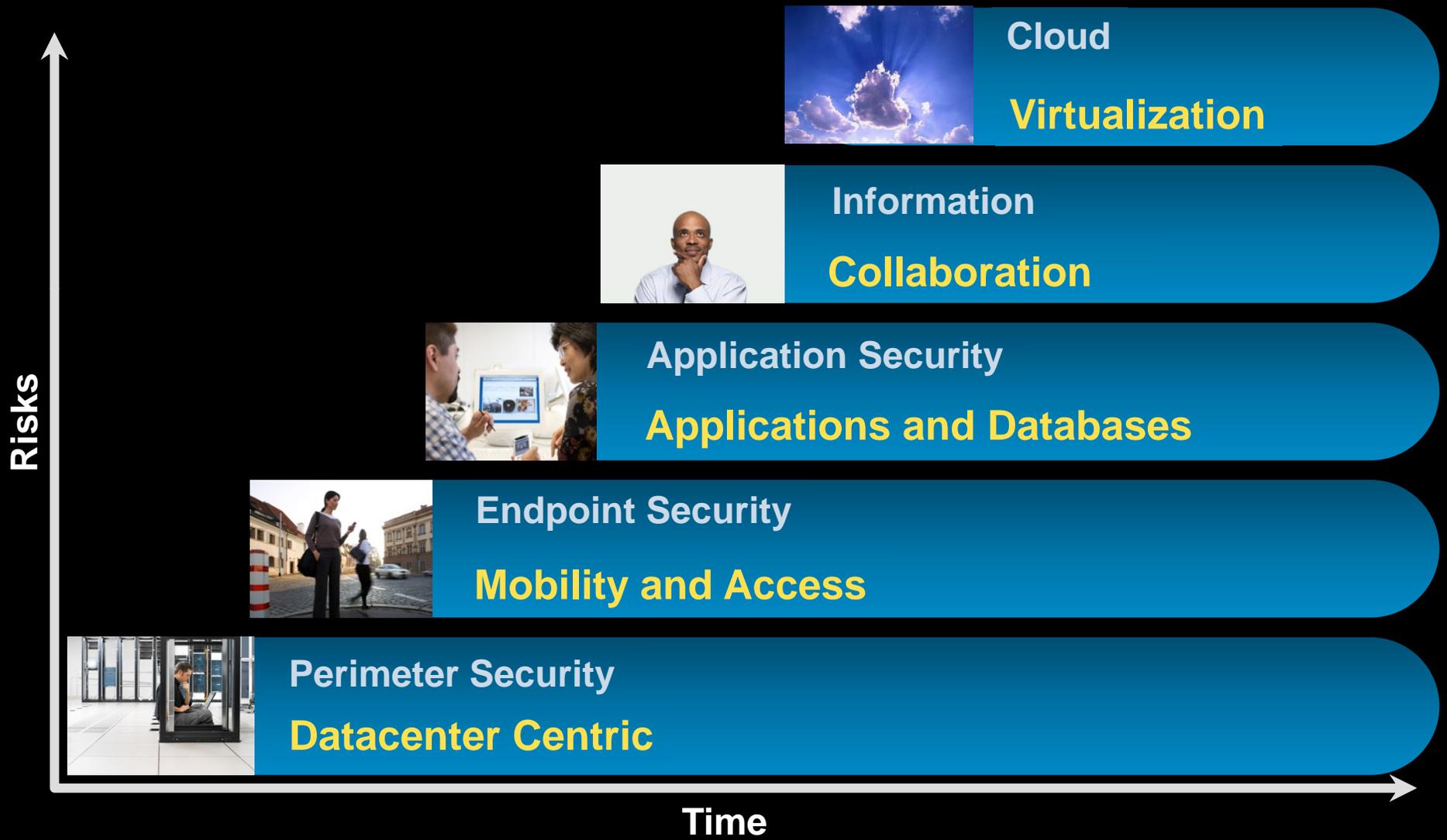


“Those who cannot learn from history are doomed to repeat it.”

~ George Santayana

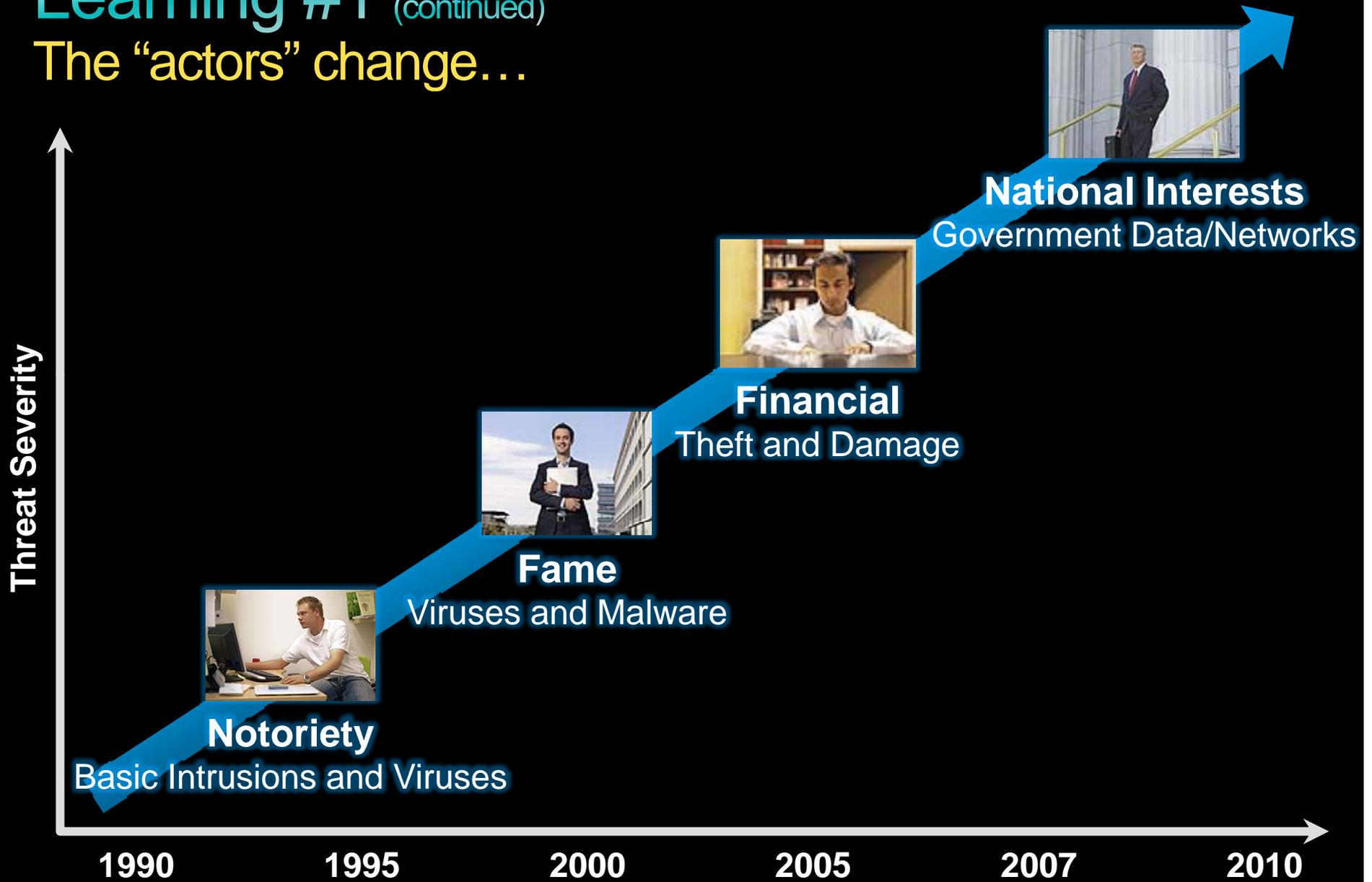
Learning #1

Once we have a handle on something, it changes...



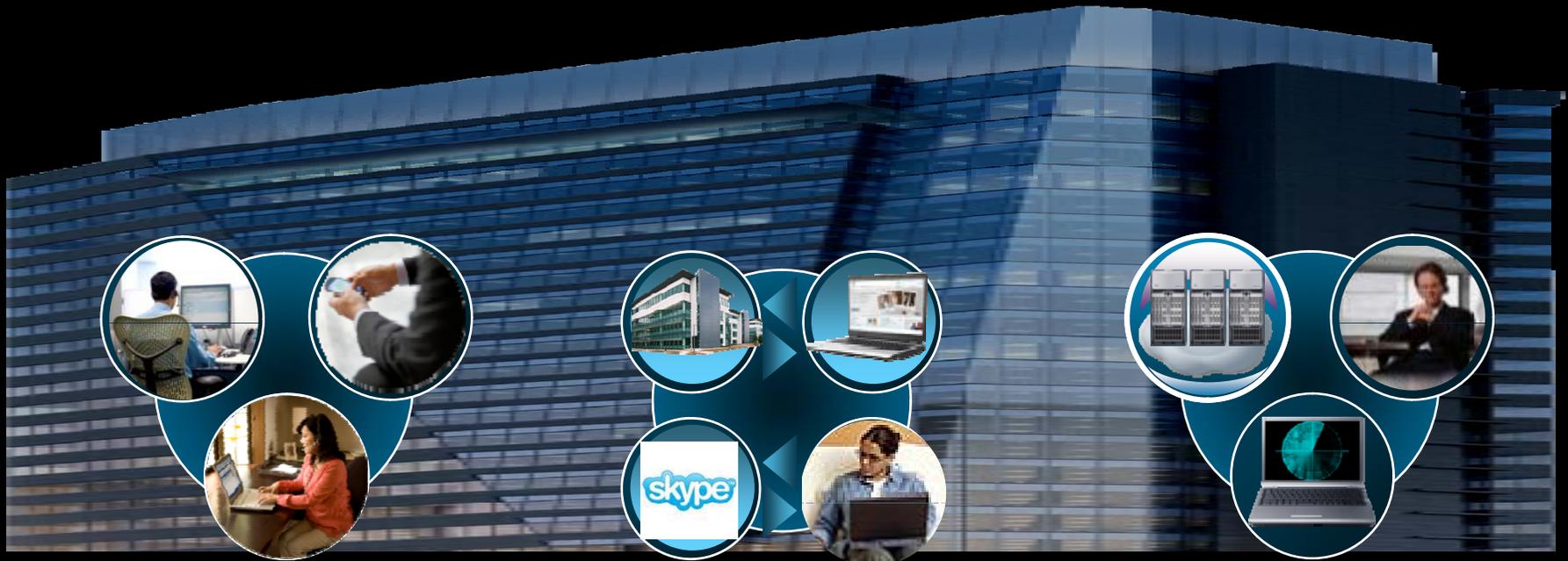
Learning #1 (continued)

The "actors" change...



Learning #1 (continued)

The technology changes...



US hospital stolen laptop:
14,000 patients records

400+ mobile malware threats exist,
1,000 expected by year end

Skype creates backdoor

Wireless FireSheep
makes news

New attack surface - Virtual
Machine and Hypervisor

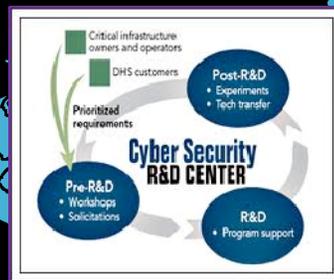
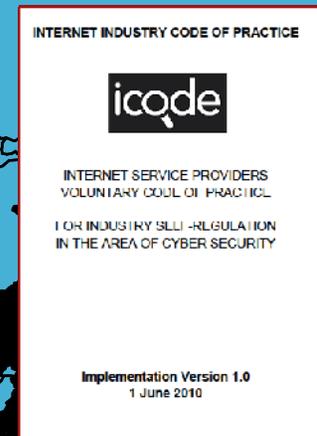
Lack of control on internal
virtual network blinds
security policies

Learning #1 (continued)

The world changes...

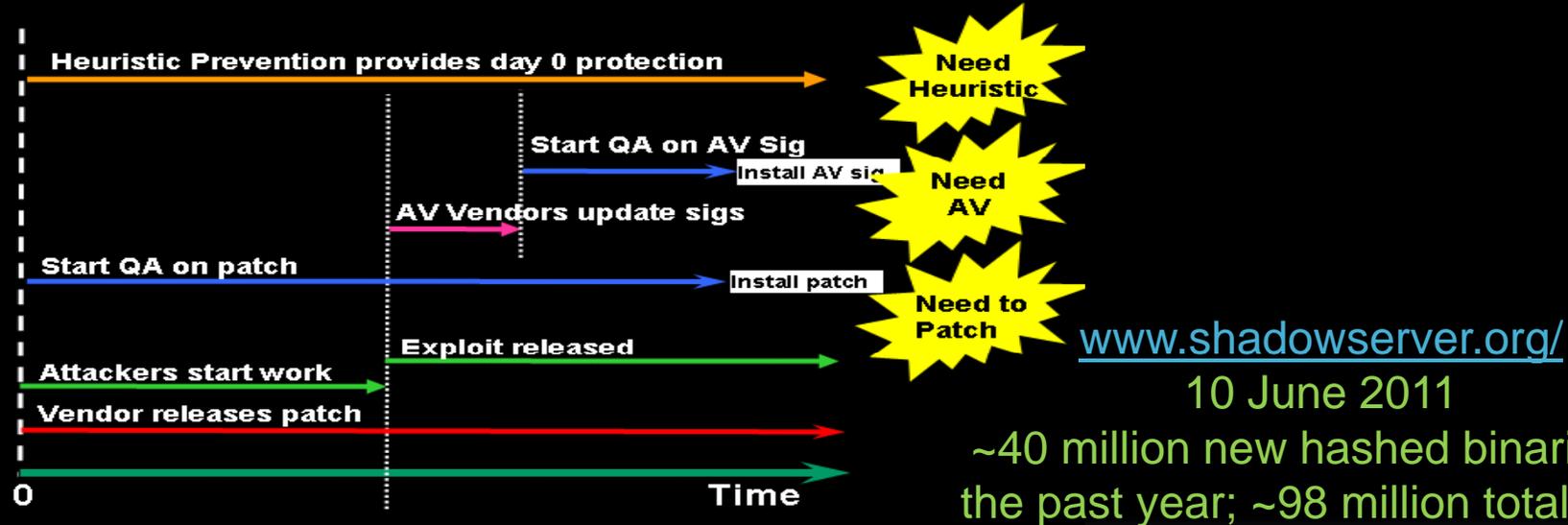


A Strong Britain in an
Age of Uncertainty:
The National
Security Strategy



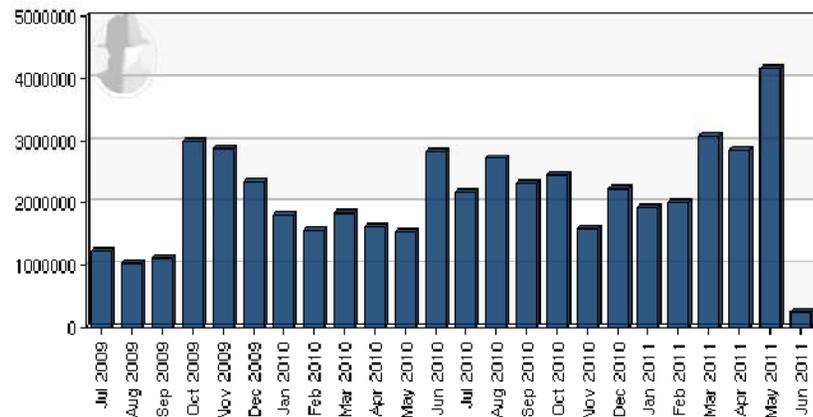
Learning #2

We rely on our practices far too long: e.g., patching, AV



~40 million new hashed binaries in the past year; ~98 million total seen

New Samples

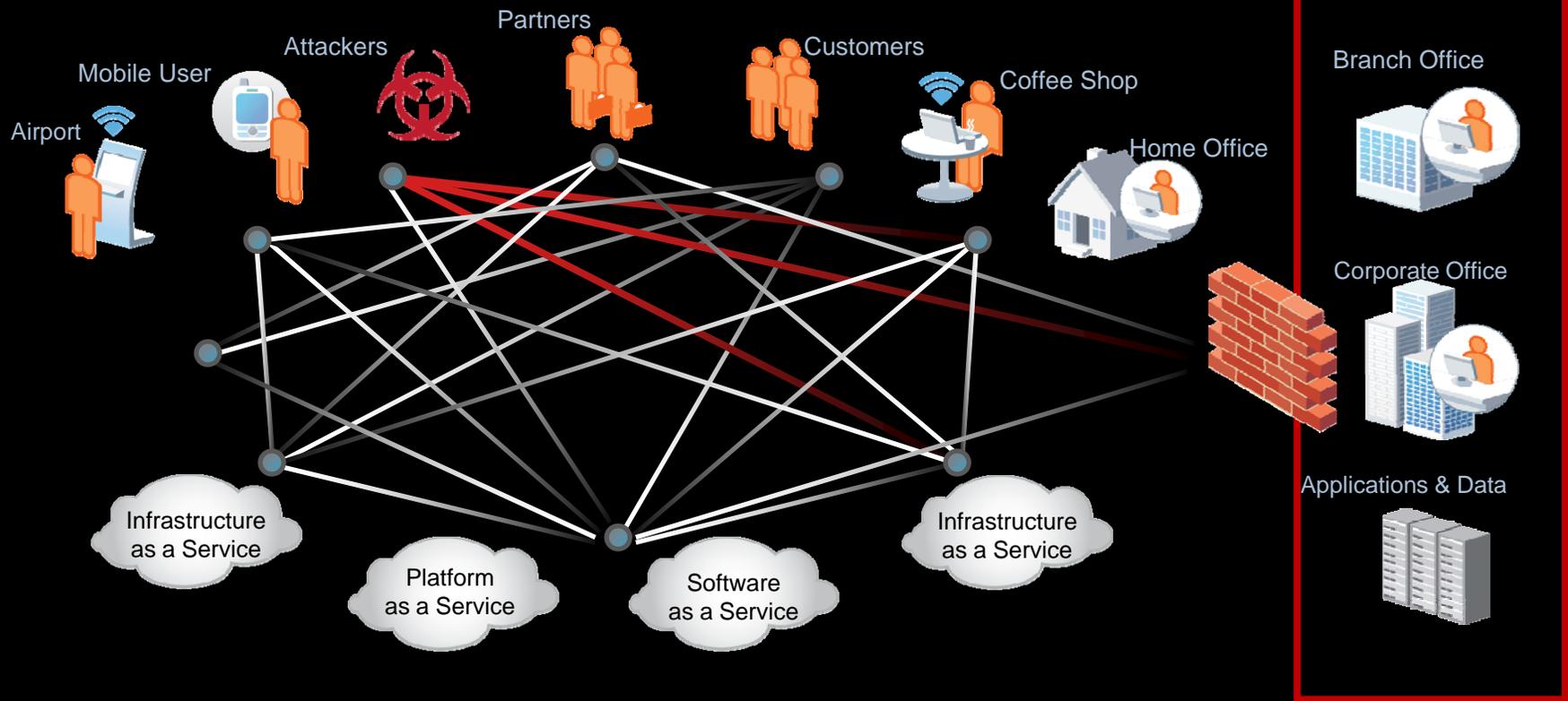


Binary Count



Learning #2 (continued)

Perimeter security



Learning #2 (continued)

Endpoint security



462 million

CHALLENGE

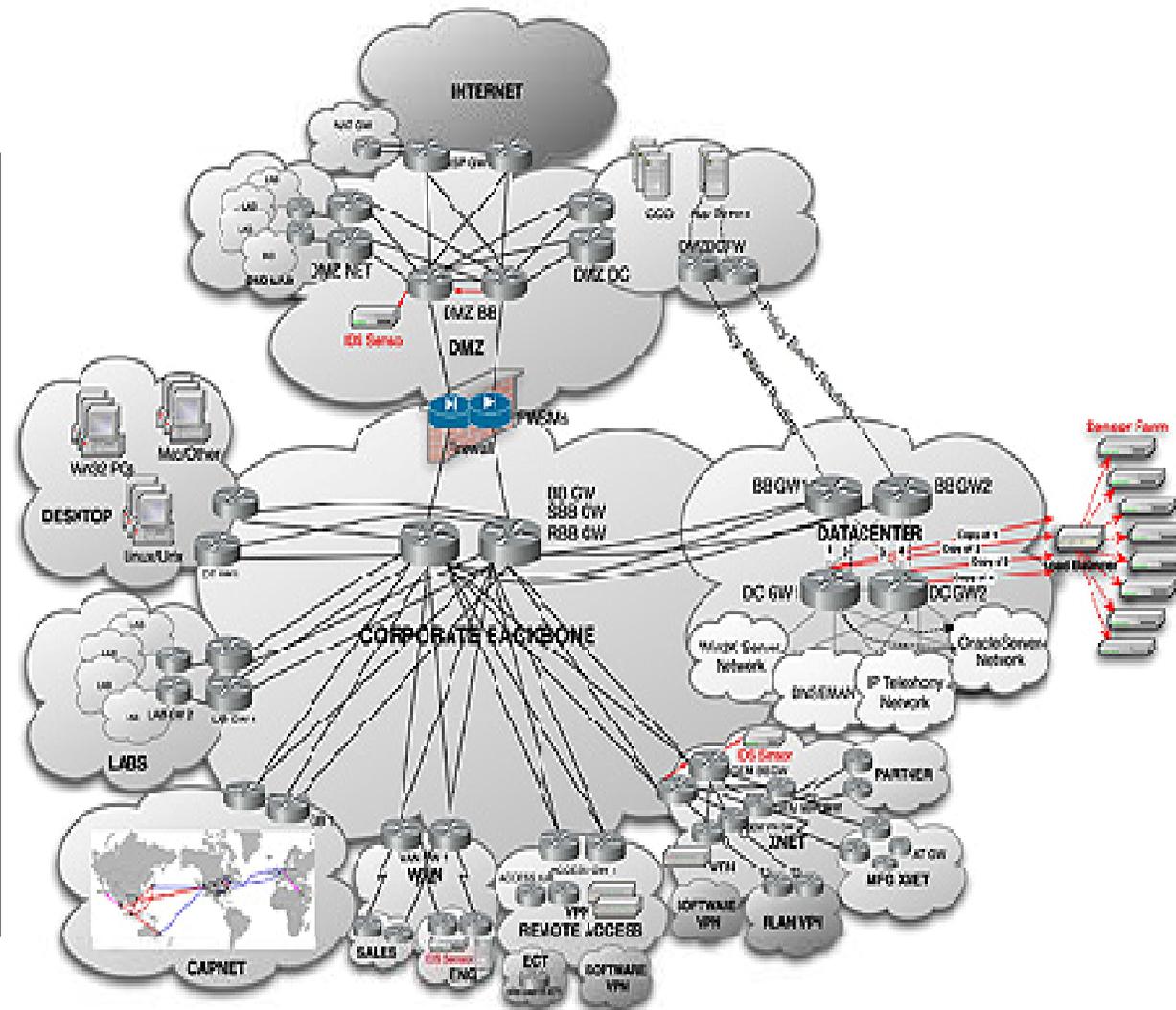
Highly mobile workers require access to network and cloud services

Variety of user-owned devices blend user and corporate profiles

Device loss/theft – highest risk of corporate data loss, compliance breach

Learning #3

We created this complex problem...



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-router
- Host-to-host
- Multi-homing

Mobile Ad-Hoc Networks

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

Miniaturization

Multi-Purpose Devices

Eradiation of Perimeters

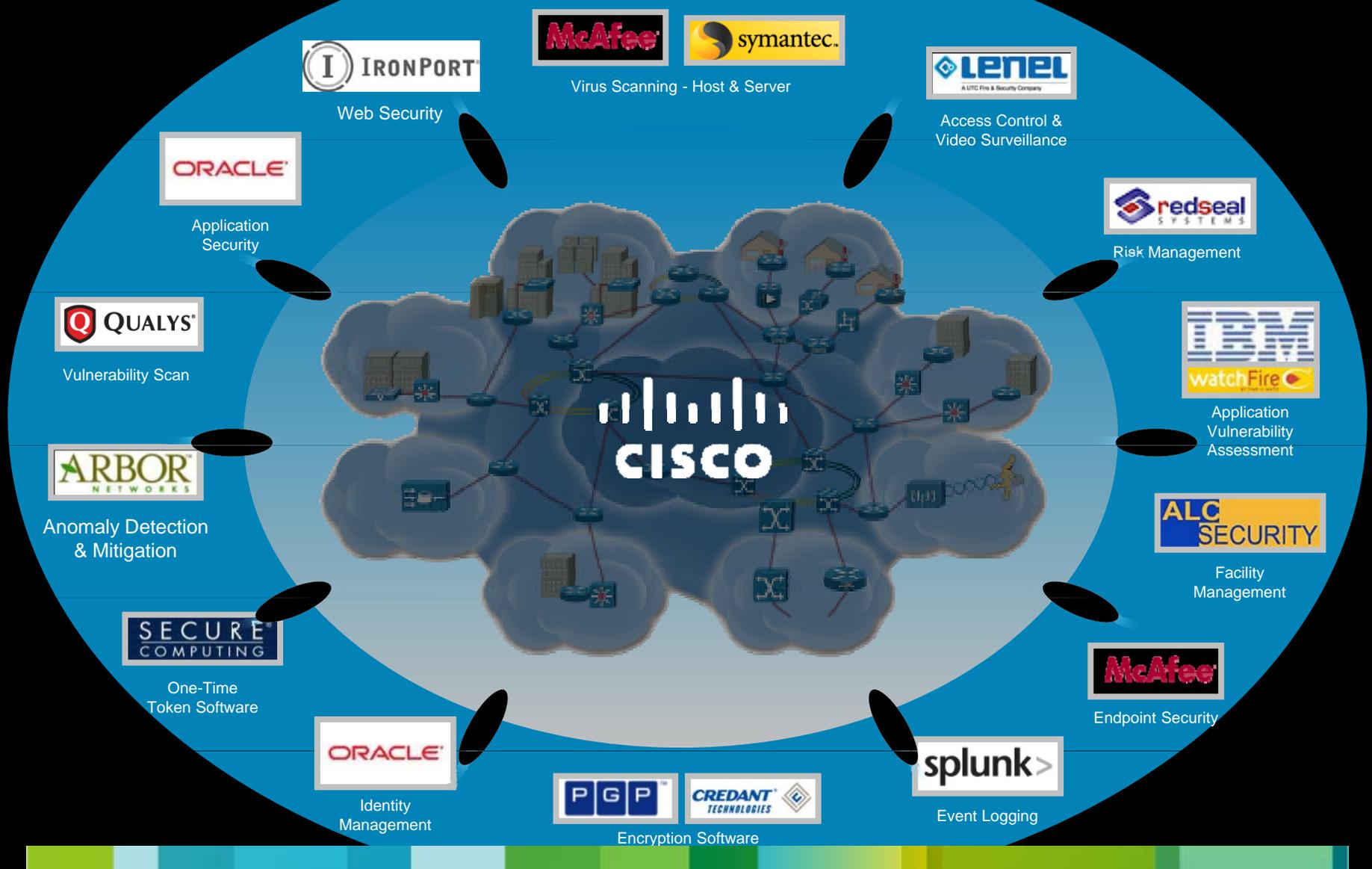
- Partners, customers, government, competitors, public

Virtualization

Cloud Computing

Learning #3 (continued)

We may even like complexity as a profession...



Learning #3 (continued)

And we are not yet motivated to change

- Expensive to Protect, Trivial to Shake Confidence
- We spend an amazing amount protecting, and it is trivial to circumvent
- We energize around electronic protection, and don't include full spectrum
- Our adversaries use our practice against us, especially when it is fixed



My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. Links and attachments want to be clicked.

So now what?





The best way to predict the future is to invent it.

~ Alan Kay

My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. Help is available, if we know where to turn and what to ask.

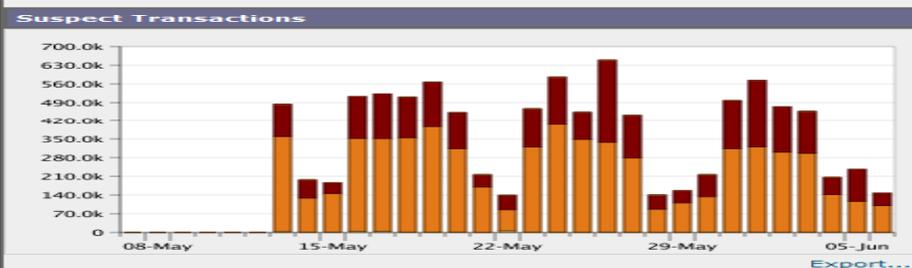
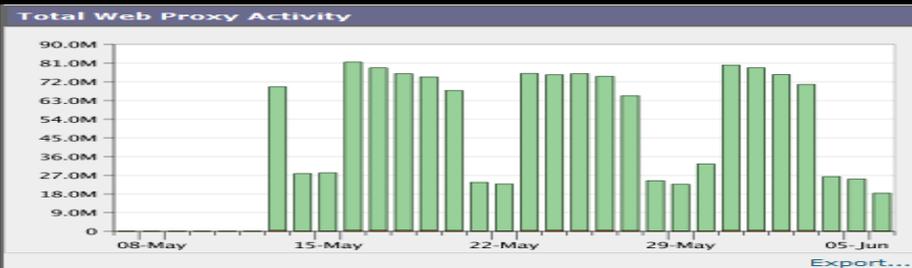
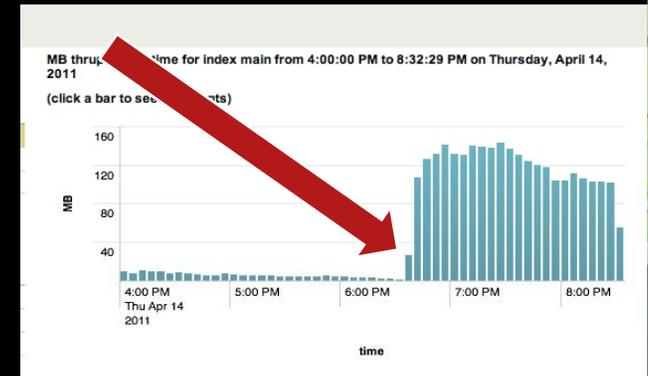
1. Users



1. Users (continued)

Attachments and links like to be clicked!

- From pilot (RTP campus) to global (phase 1)
- Total Blocked: 3.2 million+ including
 - Malware downloads
 - Browser hijacking software
 - Unwanted advertisement software
 - Botnet check-ins
 - Trojan (backdoor) connections
- Average daily log data: 30+ Gb (more than double from pilot)



Web Proxy Summary			
	%	Transactions	
Suspect Transactions	0.7%	9.5M	
Clean Transactions	99.3%	1.4G	
Total Transactions:		1.4G	

L4 Traffic Monitor Summary
No data was found in the selected time range

Suspect Transactions Summary			
	%	Transactions	
Blocked or Warned by URL Category	0.0%	0	
Blocked by Application	0.0%	0	
Blocked by Web Reputation	34.1%	3.2M	
Detected by Anti-Malware	65.6%	6.2M	
Other Blocked Transactions	0.4%	35.7k	
Total Suspect Transactions Detected:		9.5M	

My Theorems Derived from these Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. Help is available, if we know where to turn and what to ask.

2. Go Bold with Security Education and Information Sharing

Security Education

www.cisco.com/go/securityeducation

Security Intelligence Operations

www.cisco.com/security

Worldwide (change) | Login | Register | About Us

Solutions | Products & Services | On Demand | Support | Training & Events | Partner Ecosystem

Security Intelligence Operations

Inform, Protect, Respond
Early warning, mitigation, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks

Powered by IntellisShield

Severity Alert	Cyber Score	Criticality	Class	Applied Mitigation	Alerted Cisco Products
Microsoft Internet Explorer Remote Desktop Reference Access Arbitrary Code Execution Vulnerability	3.3/4	Yes	Class	Applied Mitigation	Alerted Cisco Products
Microsoft Internet Explorer Remote Desktop Arbitrary Code Execution Vulnerability	3.3/4	Yes	Class	Applied Mitigation	Alerted Cisco Products

See What's New in Critical Security
Managing and securing today's distributed and agile networks is technology (challenging) tasks about 2009 global trends and trends in the Cisco 2010 Annual Security Report. [Read the report.](#)

Enterprise Business
Report potential vulnerability in Cisco products. [Read the report.](#)

Join the Conversation

Medicine, Taxation, and Identity in Cyberspace

There are innumerable benefits to digitized recordkeeping. It can't say enough about the benefits of correlation and (collation) of information that could be gained from taking information off of paper and moving it into computers. For health information, the potential benefits are wireless and it could markedly advance a patient's well-being. The portability of data is a boon for electronic records alone, not to mention the overall value and economy of records, as well as between care and outcomes, and the effectiveness of diagnosis, treatment, and costs, all stand to benefit patients and their health.

But as health records move to digitization, some individuals are taking an opportunity to commit fraud, due to weaknesses in the system. There are risks that exist with paper records that could be mitigated by digitized records, but once health records go digital, new risks exist.

Read More

Search

Facebook | Twitter | LinkedIn | YouTube | RSS

Security Blog

blogs.cisco.com/security

Information Security Programs

Cisco is committed to empowering employee, customer, and partner security by sharing best practices and executive thought leadership.

See Cisco's internal campaign in action. [Learn More](#)

Watch Video

Data Loss Prevention | Enterprise Security | Government Security | Security Education | Security Process

Protecting intellectual property is one of the most important steps a business can take to safeguard its assets. Lost data can cost an organization millions of dollars, and

Safeguard Business Data and Resources

Smart talks about how

Cisco 2010 Annual Security Report

Highlighting global security threats and trends

2010 Annual Security Report

www.cisco.com/go/securityreport

My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. **No matter how much you think you know right now, "tomorrow" will surprise you.**
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. Help is available, if we know where to turn and what to ask.

3. Back to Basics: Simple Goals, Simple Strategy



Requires An Architectural Approach

3. 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

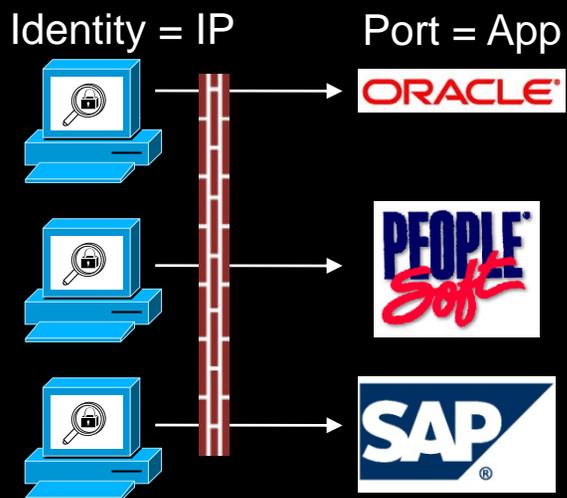
DHS Official: Cyber Attacks against Infrastructure on the Rise

By Chris Strohm

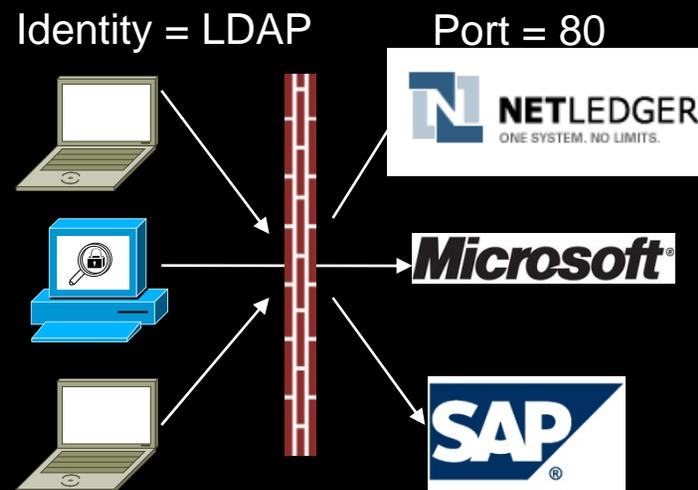
3. Solve Really Important Problems

Identity

Yesterday



Today

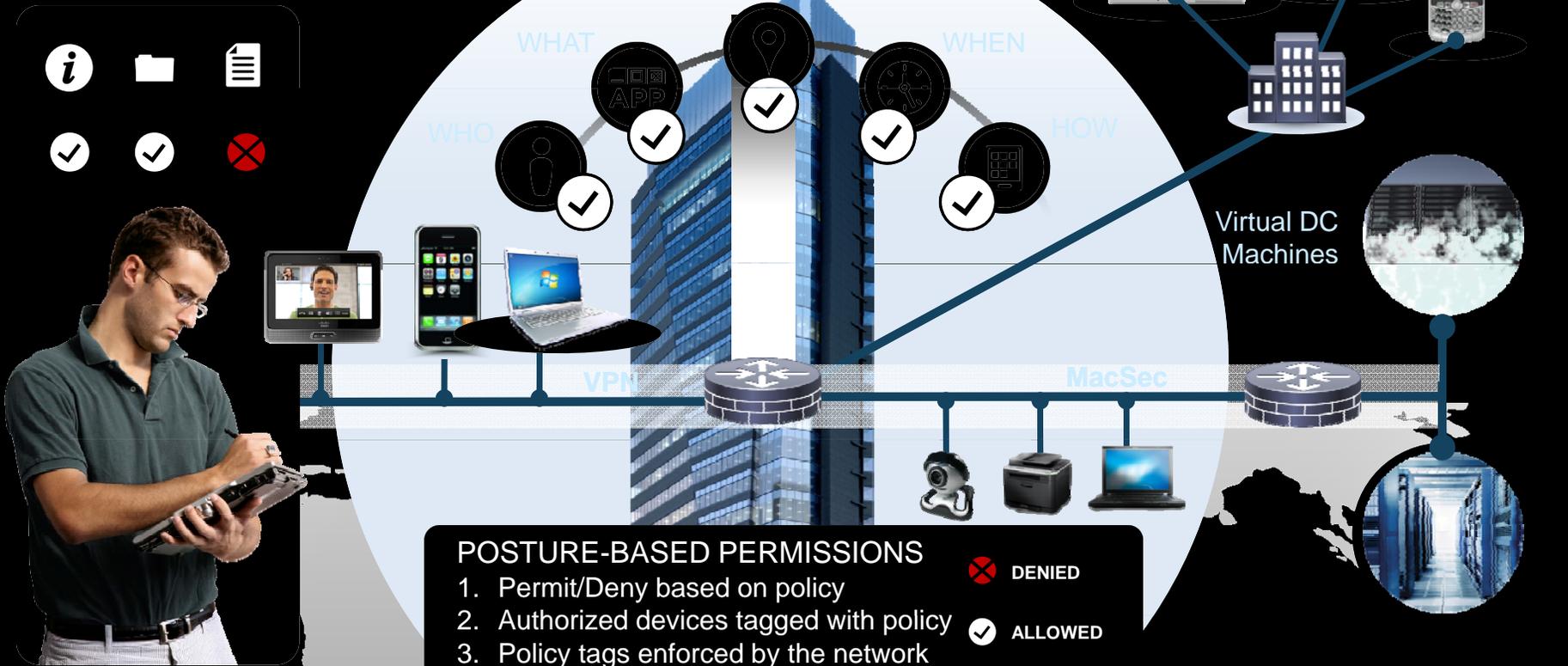


Port 80 has become a gaping hole in the firewall

Next-gen firewalls need application and identity awareness

3. Solve Really Important Problems

The Soft, Mushy, Middle



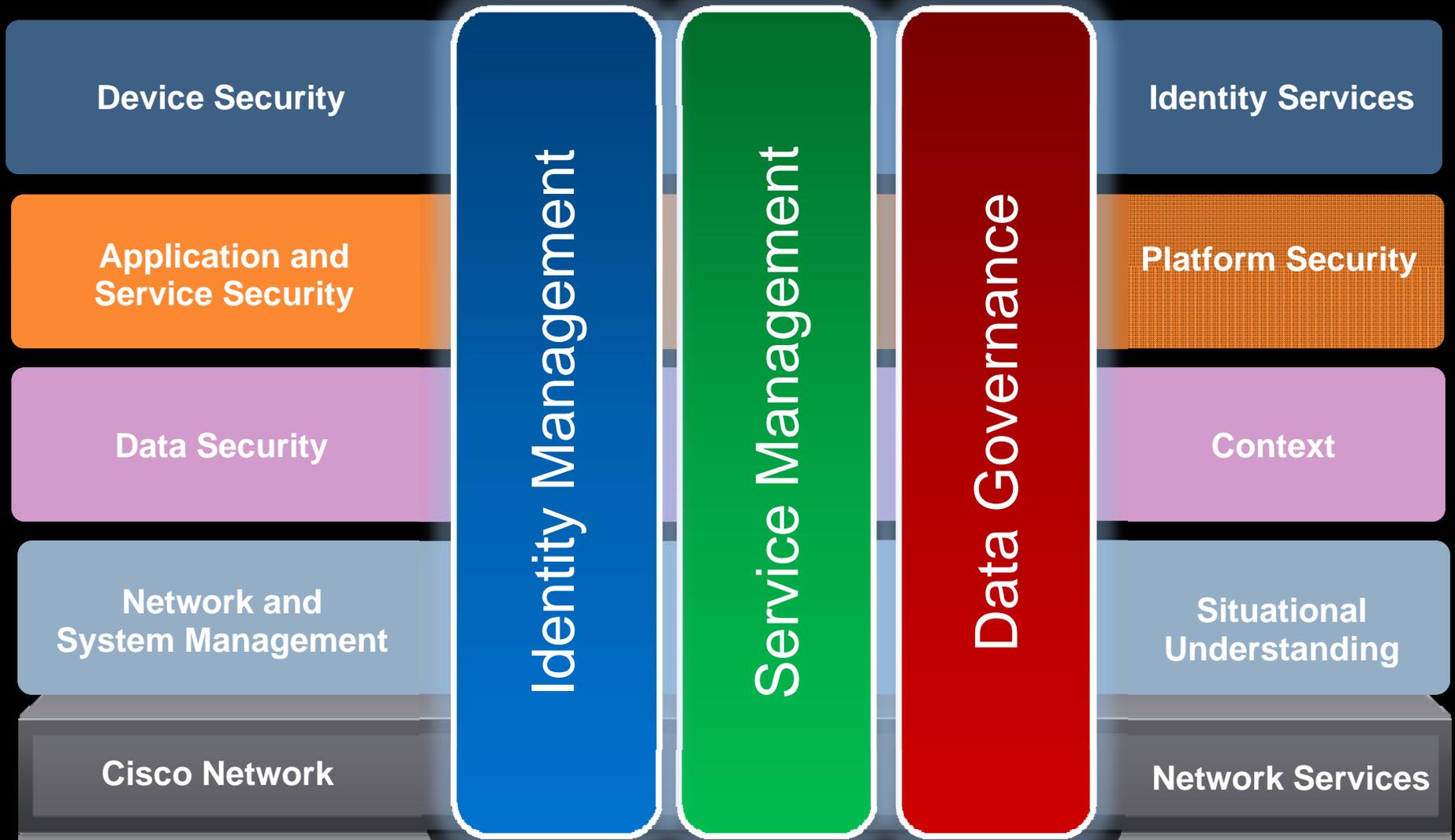
CISCO SOLUTION

Consistent identity-aware policy from any device to data center – based on **business needs**

Policy distribution and intelligence through the network

Security group tagging scales context-aware enforcement

3. Solve Really Important Problems: Architecture

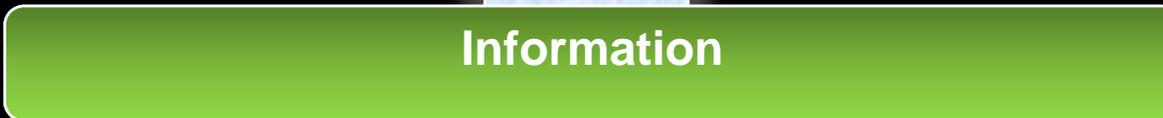


My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. Help is available, if we know where to turn and what to ask.

4. Analyze and Validate

Understanding /
Strategy /
Action



Event /
Behavior
Correlation

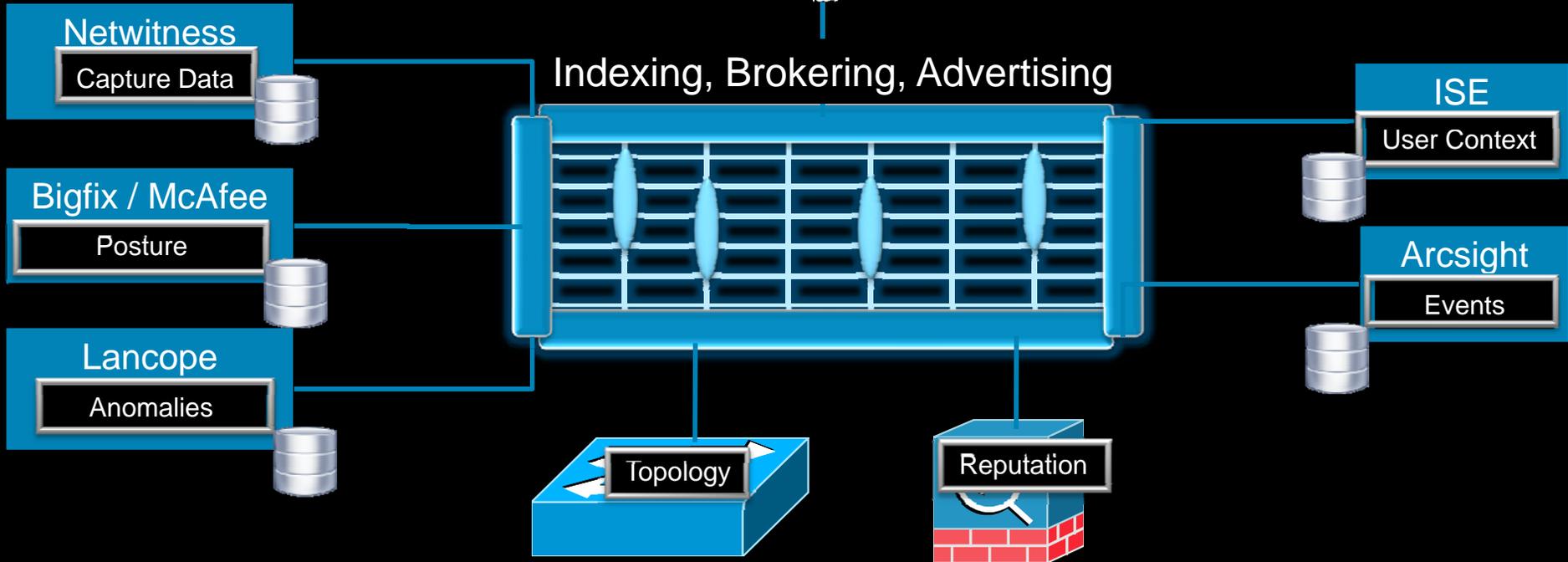
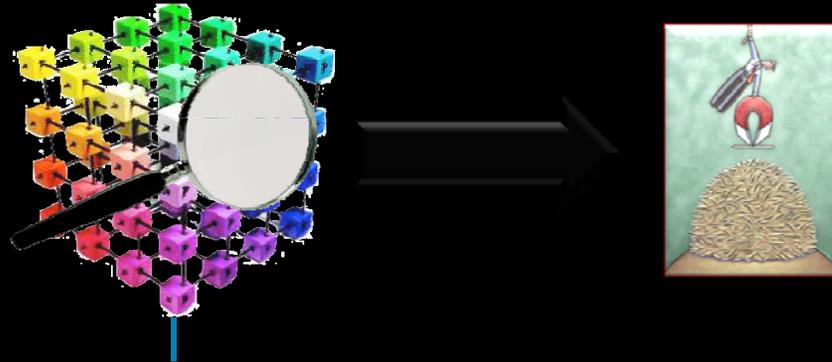


Data



“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”

4. Know What You Are Protecting



4. Have an "Eye in the Sky"

Global Visibility



CISCO SOLUTION

Largest threat analysis system - blended threat protection

700K+ global sensors
20M+ Web requests per day
35% of global email traffic
endpoint threat telemetry

Reputation, spam, malware and Web category analysis, and applications classification

My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. **The business, and the users, control our destiny.**
6. Help is available, if we know where to turn and what to ask.

5. Acknowledge the Current State

Shifting business expectations



enhance customer relationships, improve productivity, accelerate globalization

5. Acknowledge the Current State (continued)

Shifting employee expectations

60%

Don't need to be in the office; 66% will take lower paying job for it (10%)

45%

Would work an extra 2-3 hours per day if allowed to do so remotely

59%

Want to use their personal devices at work

45%

Of IT staff are unprepared to make workforces more mobile

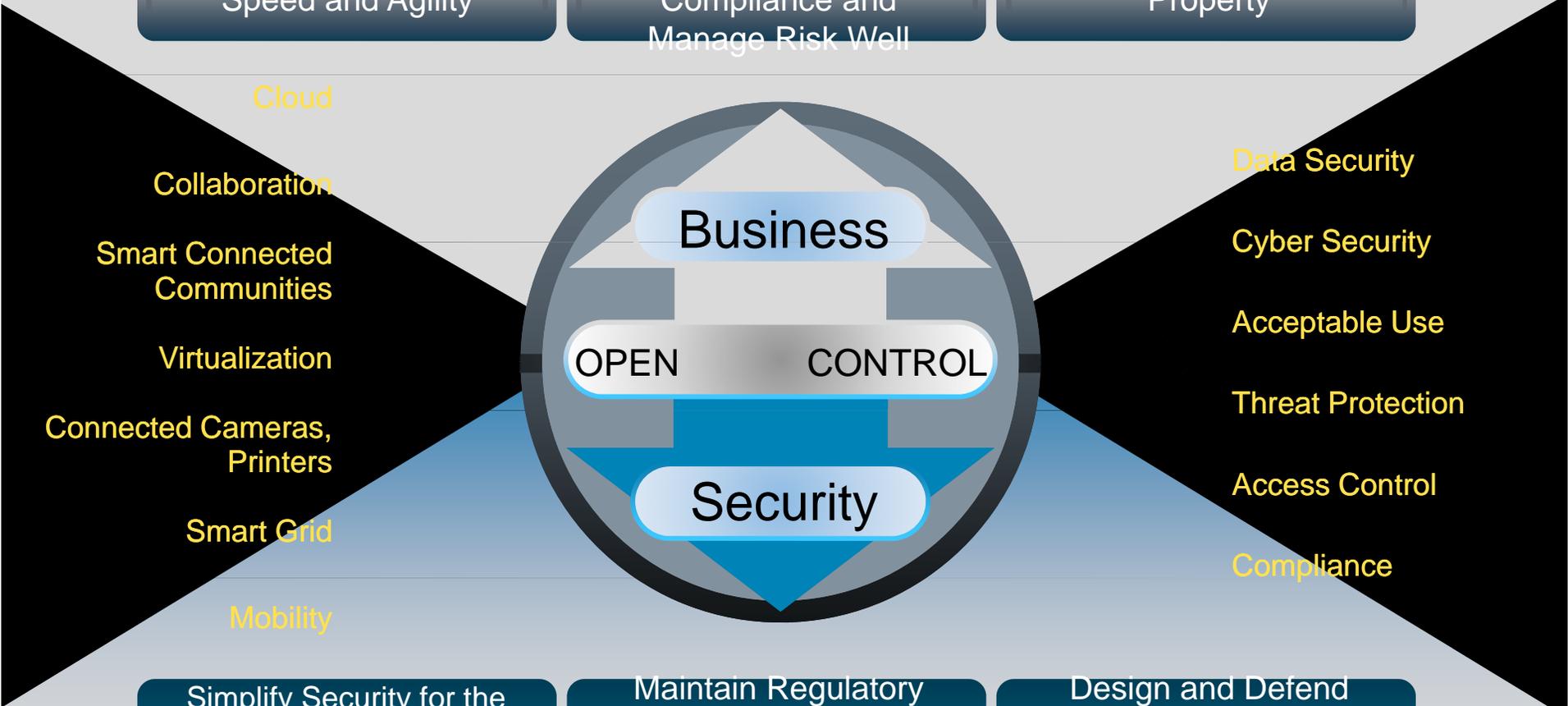
57%

Of IT staff said security is the biggest challenge for mobile workforce



5. Harmonize Business and Security (continued)

Enable Business Speed and Agility Maintain Regulatory Compliance and Manage Risk Well Protect Intellectual Property



Simplify Security for the User, the Business, and the Operations Maintain Regulatory Compliance and Manage Risk Well Design and Defend for Unpredictable Threats

My Theorems Derived From These Lessons

1. All the security controls in the world cannot stop ignorant, imaginative, and/or malicious users from hurting themselves or the organization.
2. Most people don't have a clue about computer security, and don't want to know... yet we must try.
3. No matter how much you think you know right now, "tomorrow" will surprise you.
4. You can't secure what you can't see, except luckily. Turns out, luck isn't much of a strategy.
5. The business, and the users, control our destiny.
6. **Help is available, if we know where to turn and what to ask.**

6. Bad News Does Not Get Better With Age

Swede Charged in Alleged Attacks on NASA, Cisco



The Justice Department claims a Swedish man ran one of the largest Internet hacking attacks, which compromised a wide variety of universities, companies, government facilities and international organizations -- but the man could end up beyond the reach of U.S. law.

Security Industry

RSA SecurID authentication tokens hacked

Published: June 7, 2011 at 1:57 PM

Sony Pictures says LulzSec hacked 37,500 user accounts, not 1 million

June 9, 2011 | 3:02 pm



Cisco Live 2010 attendee list hacked

Cisco notifies customers their registration info was compromised in security breach

By [Tim Greene](#), Network World
July 08, 2010 04:31 PM ET

[Comment](#) [Print](#)

Someone hacked the list of attendees for the recent [Cisco Live 2010](#) users' conference, a security breach that led Cisco to notify the customers as well as a broader group who have dealings with the company.

I.M.F. Reports Cyberattack Led to 'Very Major Breach'

By [DAVID E. SANGER](#) and [JOHN MARKOFF](#)
Published: June 11, 2011

WASHINGTON — The [International Monetary Fund](#), still struggling to find a new leader after the arrest of its managing director last month in New York, was hit recently by what computer experts describe as a large and sophisticated cyberattack whose dimensions are still unknown.

[f](#) RECOMMEND

[t](#) TWITTER

[e](#) SIGN IN TO E-MAIL

[p](#) PRINT

6. Get to know your friendly CERT and Law Enforcement teams – make new friends



GovCERT AUSTRIA



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?





EXPERIENCE

Experience is what you get, when you didn't get what you wanted.

Thank you.

