





Security Challenges - Today and Tomorrow

Christopher Burgess
Director and Senior Security Advisor
Corporate Security Programs

chrburge@cisco.com

[@BurgessCT](#) (Twitter)

www.cisco.com/web/about/security/cspo

Threat Histories and Futures

Attacks focused on:

Operating Systems

- Microsoft OS
- Linux
- Solaris

Attacks focus on:

Applications

- Databases
- Application suites
- 3rd-Party applications
- Web applications

Attacks will focus on:

Next Generation Technologies

- Collaboration suites
- Virtualization technology
- Networks themselves
- SaaS & ITaaS

Yesterday

Minutes to Hours

Today

Seconds to Instant

Tomorrow

Instant to Persistent

Attackers were:

Minimally Experienced

- Mischievous
- After notoriety
- Using virus payloads via email

Attackers are:

Well Trained

- Well resourced
- Professional (\$) gain
- Delivering malware via websites

Attackers should be:

Seasoned

- Attacks against prime providers
- Attack multiple computers with a computer
- Polymorphic

Perimeter

Pervasive

Data Centric

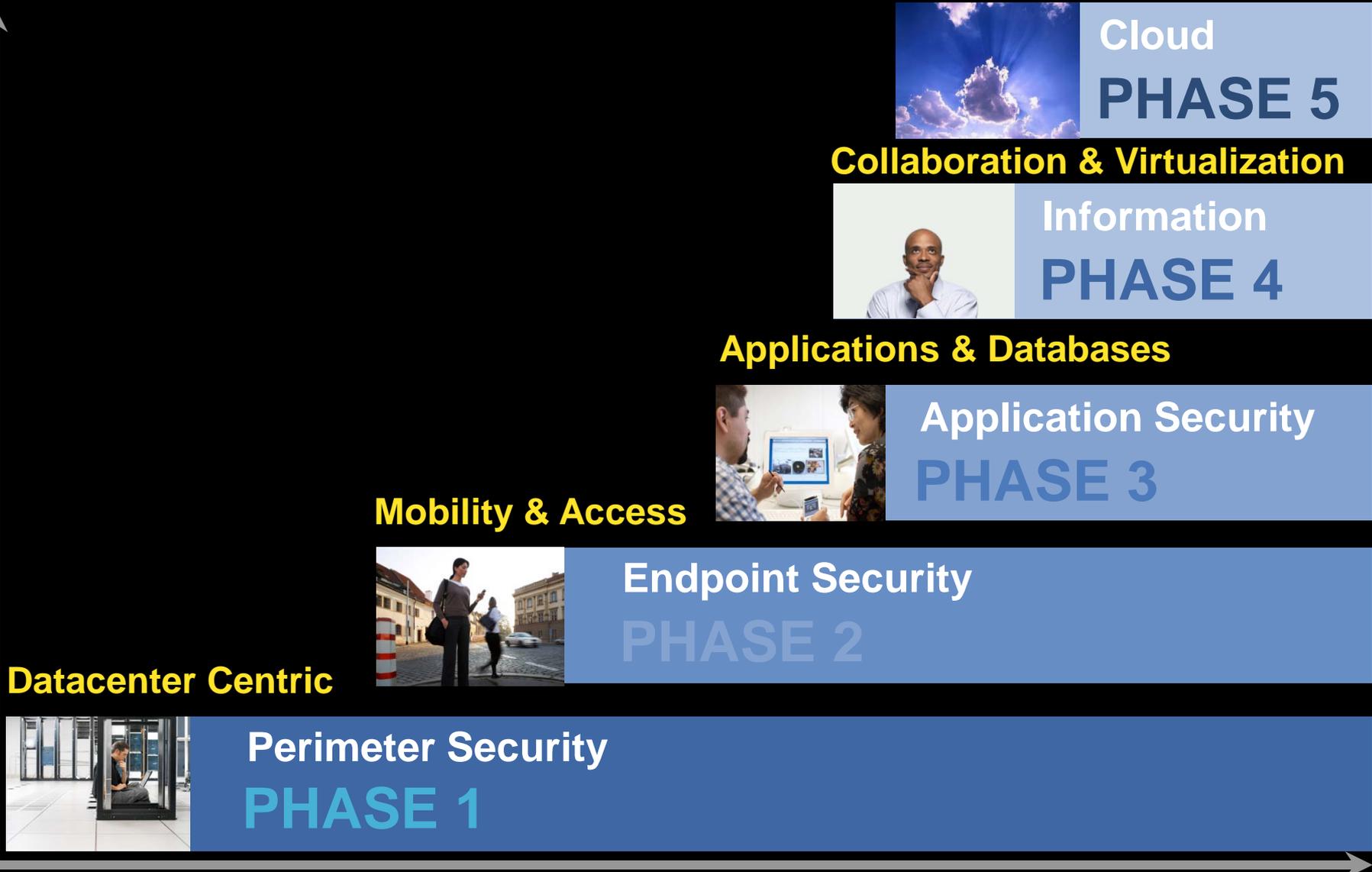
User Centric

Hobbyists

Professionals

Significant Security Challenge: Transitions

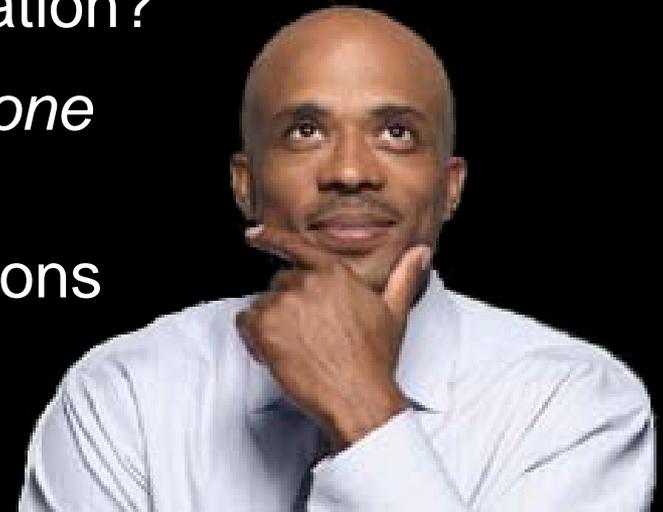
Risks



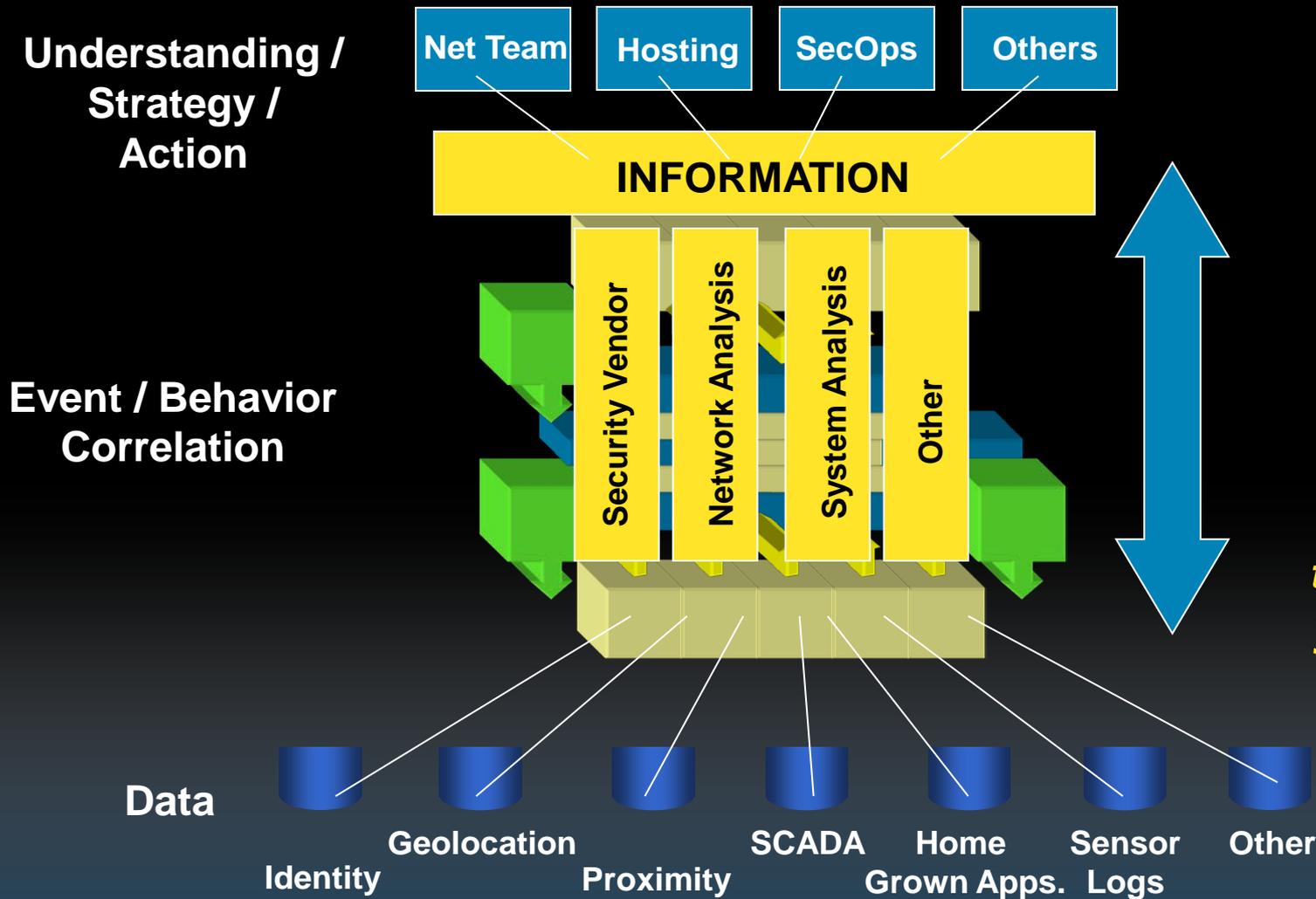
Data

The Key To Understanding Your Environment

- What is on my network?
- Where is it on my network?
- How did it get on my network?
- What condition is it in?
- Who is/should be using it?
- Where does my network “go?”
- Who is *really* in control of my information?
- How do I manage security when *no one* is in control of my data?
- Do I design for compromised operations or try and assure clean operations?



Data Analytics Is The Future



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

~ or ~

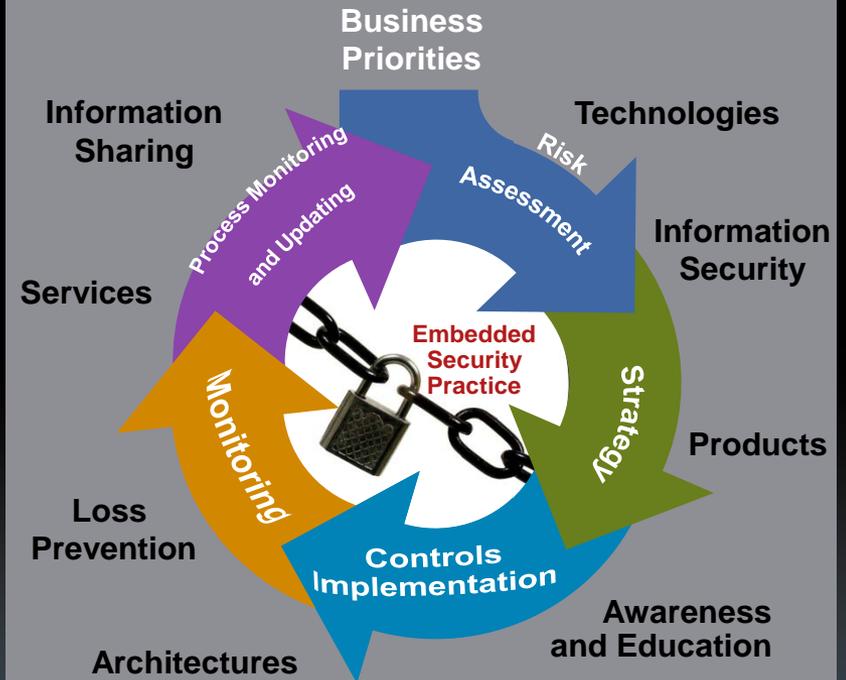
“I don’t know the questions yet; let’s look at the data.”

Defining Your Security Footprint

Security Includes Everyone



Security Includes Everything



No Exceptions

People: **Your Greatest Security Asset**

“At Cisco, we are all accountable for our actions and rewarded for leadership behaviors that help keep our customers, partners, suppliers, and ourselves as secure as possible. Awareness and education are vital for our success.”

~ John N. Stewart
Vice President and Chief Security Officer

The Success of Any Organization...

Ultimately is based on individuals' actions and choices

Goal: Employees Understand That Everyone Is Responsible for Security

- Establish a culture of security
- Recognize that senior leaders set the tone for the culture of an organization
- Develop a visible and focused awareness and education program
- Institute incentives and recognition for employee security leadership



Security is Leader-led...



“Security starts with me, the CEO, down to the individual contributor level... it’s mandatory.”

John Chambers
Chairman and CEO

“Security has to be in every aspect of every thing that we do. It’s fundamental to the way we do business.”

Brad Boston
SVP, Global Government Solutions



“Security must be built into every aspect of our systems architecture and be seamlessly compatible with our business architecture.”

Rebecca Jacoby
Chief Information Officer

...Awareness and Education Driven...

- Pervasive awareness and education programs
- Cross-collaborative efforts of constituents
- Policies, guidelines and essential practices
- Rewards for exemplary security related behavior
- Compelling set of marketing activities and communications

Be A Security Champion



Training & Education



Marketing Collateral



Award-winning Programs

We Are The Targets



Creative Communications

...And Accountable By Everyone

- **Cisco Code of Business Conduct is designed to deter wrongdoing and promote:**

Honest and ethical conduct

Full, fair, accurate, timely, and understandable disclosure in reports and documents that Cisco files with or submits to government agencies and in other public communications

The protection of Cisco confidential and proprietary information, as well as our customers' and vendors'

Compliance with applicable governmental laws, rules, regulations

The prompt internal reporting of violations of this code

Accountability for adherence to this code

- **Information Security**

Protecting Cisco resources is paramount to the company's success. Each employee is required to know, adhere to **Cisco Information Security policies**.



Process: **Your Path for Success**

“Security process is the execution of security strategy using technology as the enabler and people as implementers. It is absolutely critical as it validates business strategy.”

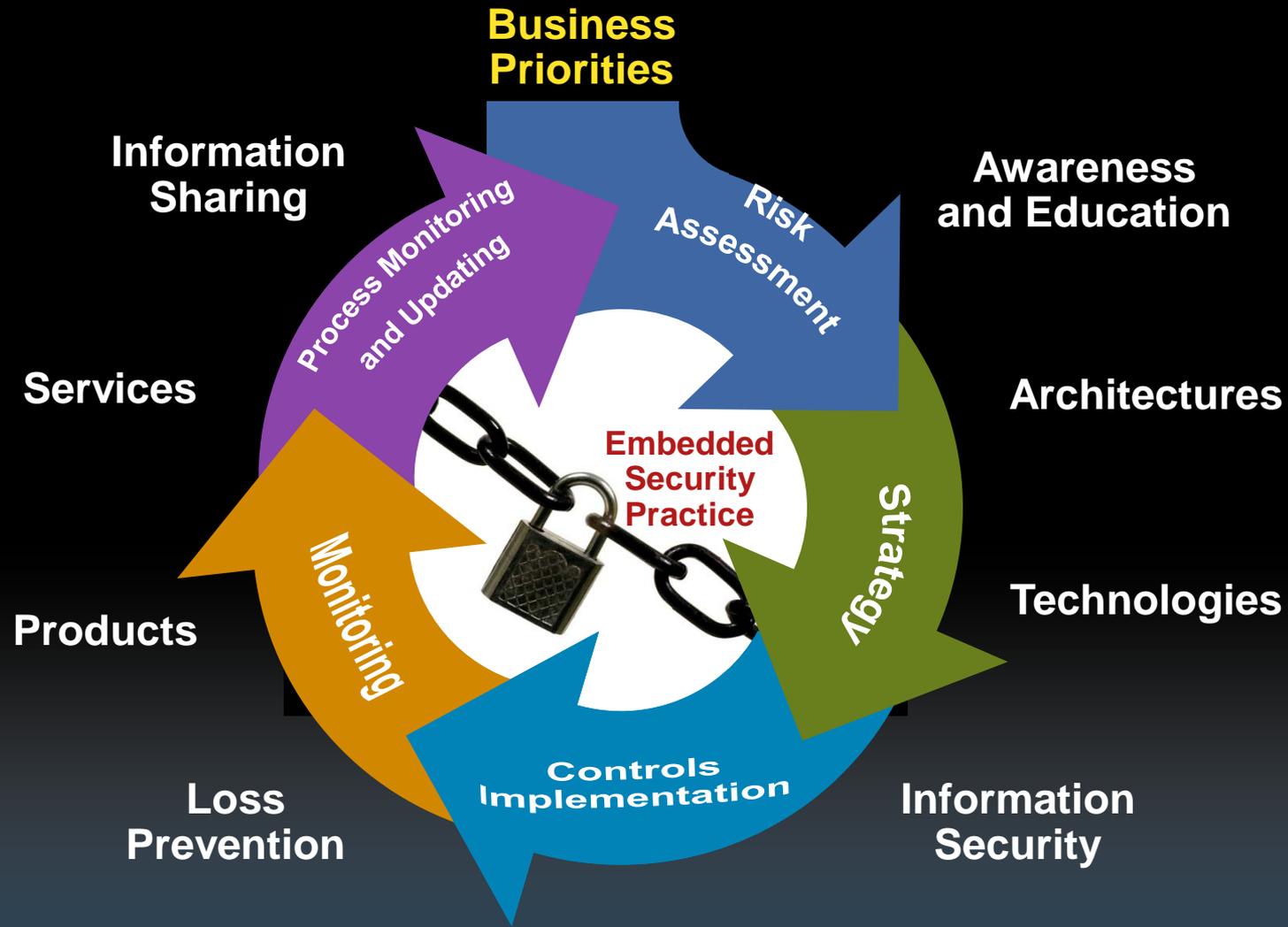
~ Nasrin Rezai
Cisco Director of Information Security

A Security Process...

- Starts with the company's business strategy and culture
- Illustrates the requirements necessary to minimize risk, maximize business efficiency
- Is the realization of security strategy in support of the business strategy
- Must be dynamic and in a constant state of balance as it evolves with the business strategy



...Identifies, Measures, and Controls Risk...



A cyclic, multistage, multifaceted approach
focused on incremental continuous improvement

...And Is An Overlooked Factor for Success

- A security process needs to be well-defined, measurable, and take you from where you are to where you want to be
- To be effective, security processes must also:

Be optimized for speed and performance

Add value at every step and in all dimensions

Be richly connected into all aspects of the business

Have metrics embedded within the process

Have process control systems:



**Process is the path for success
that leads people and technology to excellence**

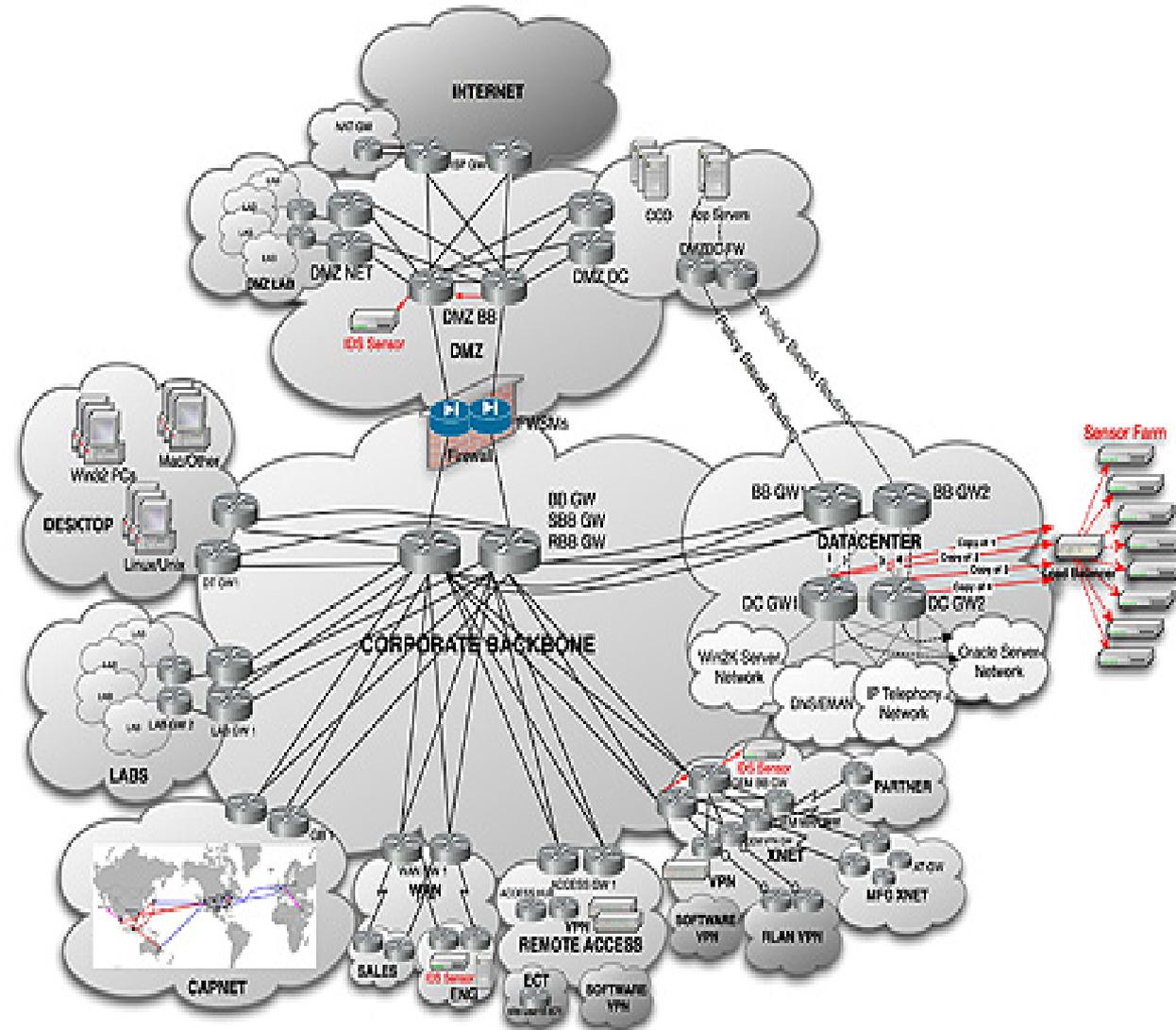
Technology: **Your Tools for Defense**

“It is important to invest in protective measures commensurate to the value of the asset being protected.”

~ Richard Power and Christopher Burgess
“Secrets Stolen, Fortunes Lost”
Syngress, March 2008

Technology & Users Aren't The 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-router
- Host-to-host
- Multi-homing

Mobile Ad-Hoc Networks

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

Miniaturization

Multi-Purpose Devices

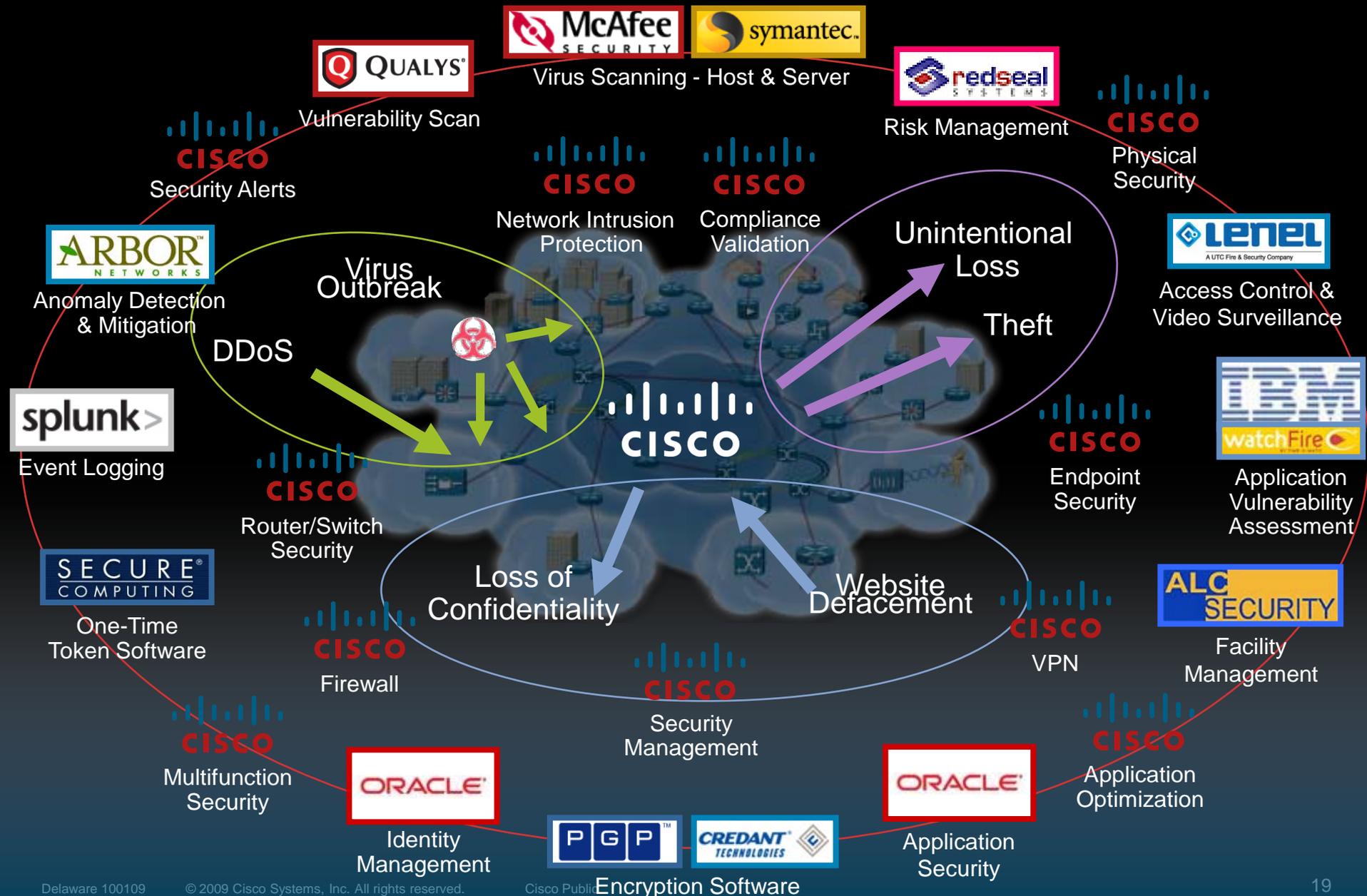
Eradiation of Perimeters

- Partners, customers, government, competitors, public

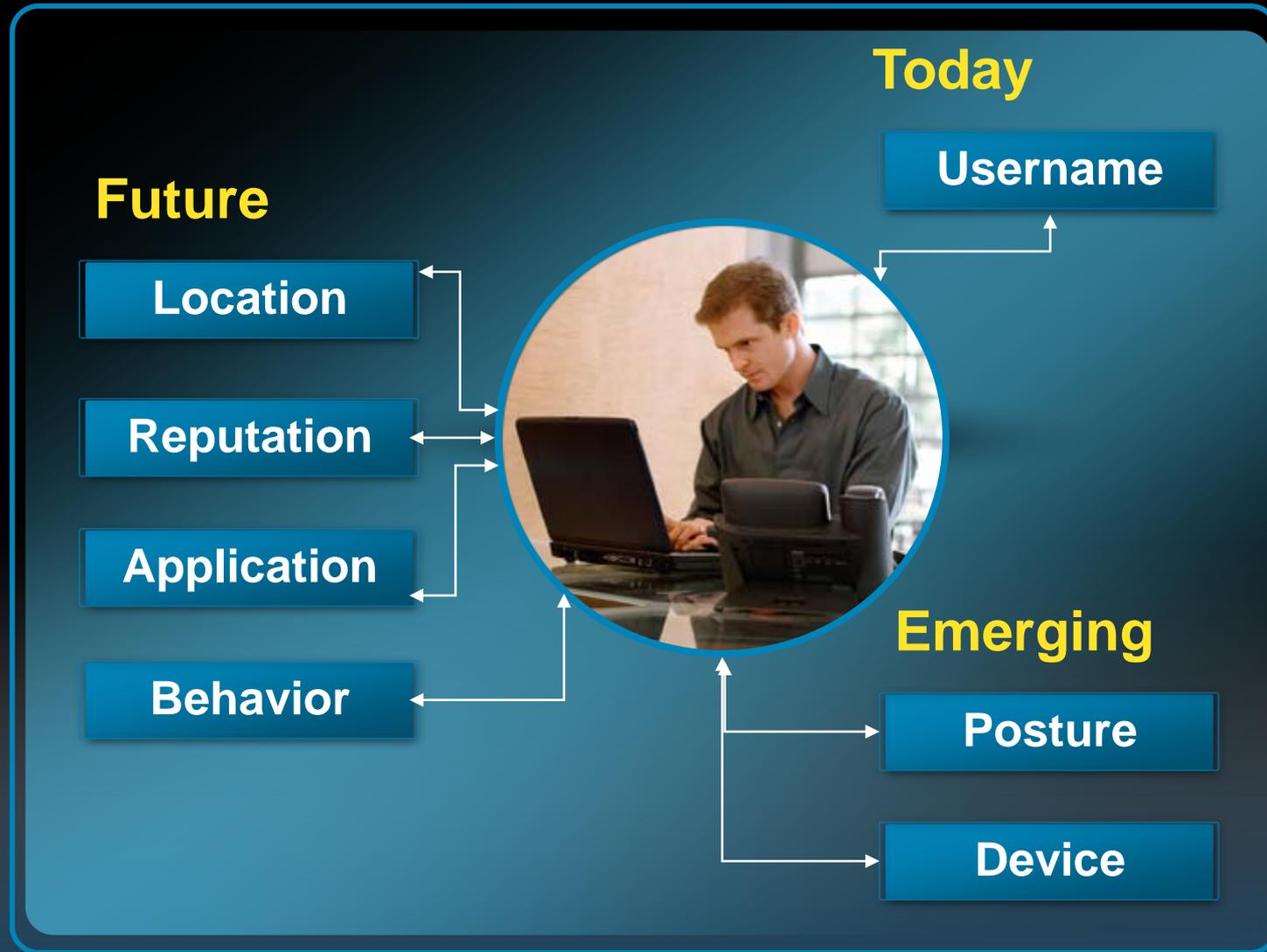
Virtualization

Cloud Computing

Technology Integration Is Complex

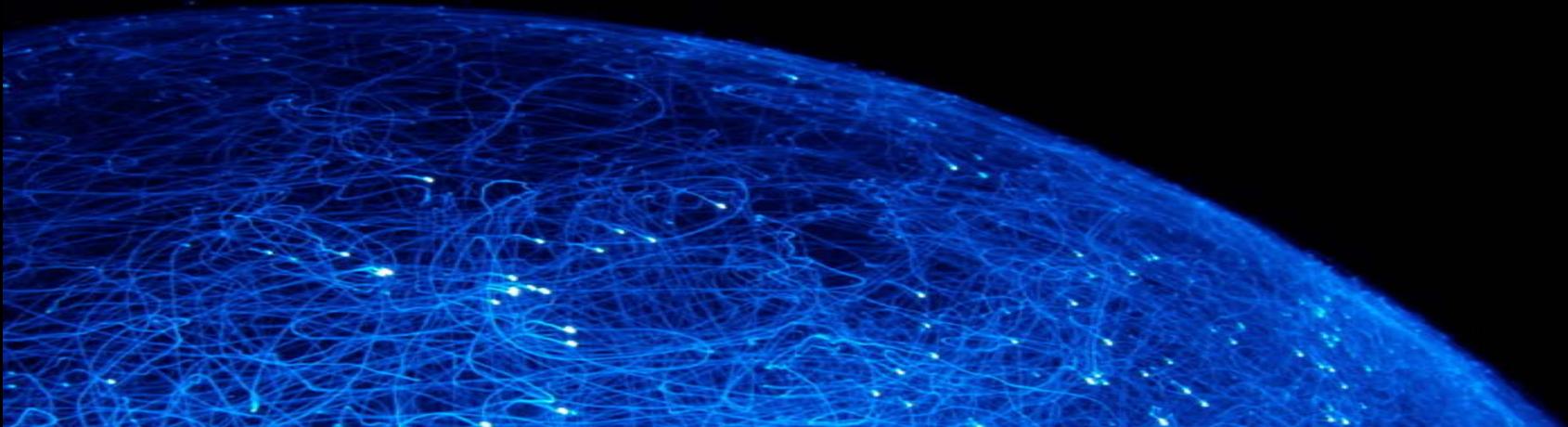


Identity Attributes



If We Have Good Identity...

- In general, **people behave more appropriately** when they believe somebody or something is watching them
- **We can be confident** in who did what, good or bad
- **Confusion** over insider, outsider, hacker, organized crime, nation state **could go away**



What Is The Problem?

To date, the 'Web 2.0' and online application communities generally **have not been closely engaged** with the traditional computer security nor network operational security communities.

This lack of engagement can have negative consequences for those who depend upon these applications – **increasingly, this means enterprises.**



Collaboration Isn't Just Useful...



...it's essential.”

Collaboration / Web 2.0 Security Threats

- **Social Networking, Privacy, and Symmetric Trust**

 - Where is the perimeter – and which do you care about?

 - How do I truly know it's you?

 - Isn't inherent openness / social collaboration the inverse of privacy?

- **Digital Rights Management (DRM)**

 - Who "owns" the data?

 - How do you protect your intellectual property?

- **Malware Installation and Spread**

 - How do we protect ourselves on this "super" distribution channel?

 - By volunteering personal information, aren't you putting it at risk?

- **Root Cause**

 - How do we understand what is going on?

 - How do we identify the culprit?

Social Media

Does Not Change Your Personal Compass

*Abide by
the rules*

*You are
responsible*

Add value

Be mindful

Be honest

Be respectful

Be yourself





Concluding Thoughts



Key Considerations / Takeaways

- **We Share Common Challenges, Threats**
- **An Integrated Business Security Strategy Unites Business and Security Requirements, and Is All-Encompassing**

Security Starts At the Top, Touches Everyone, Everything

Is a cyclic, multistage, multifaceted approach focused on incremental continuous improvement

Requires proactive and reactive preparation

Is not a cost center, but a business enabler

- **Dynamic Business Requirements, Capabilities, and Challenges Require New Approaches to Security**

Social Media Changes the Game, Not Your Personal Compass

Combining People, Process and Technology achieves the best security posture and drives efficient business results

Questions?



