



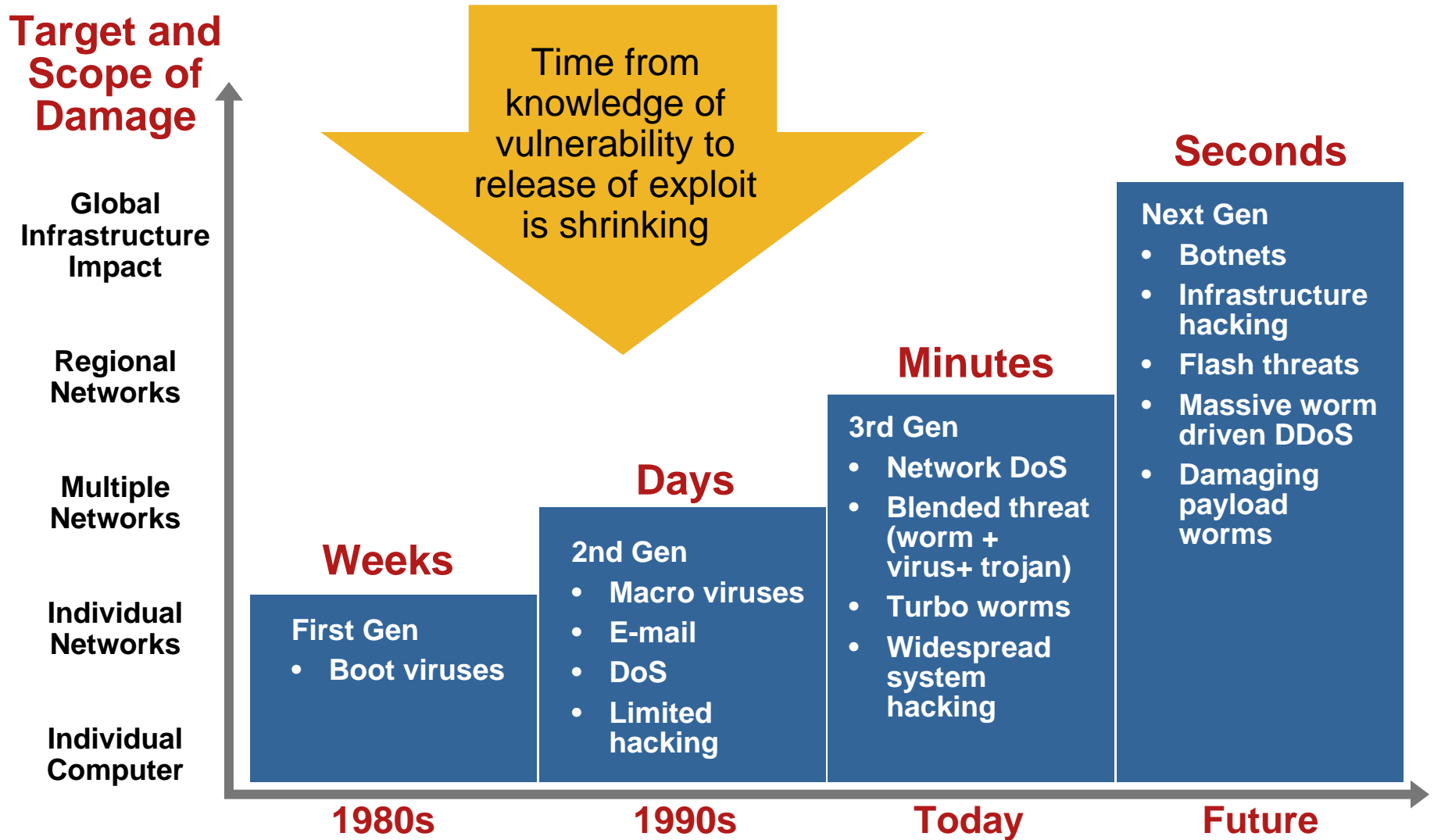
Cisco IT Executive Presentation Security



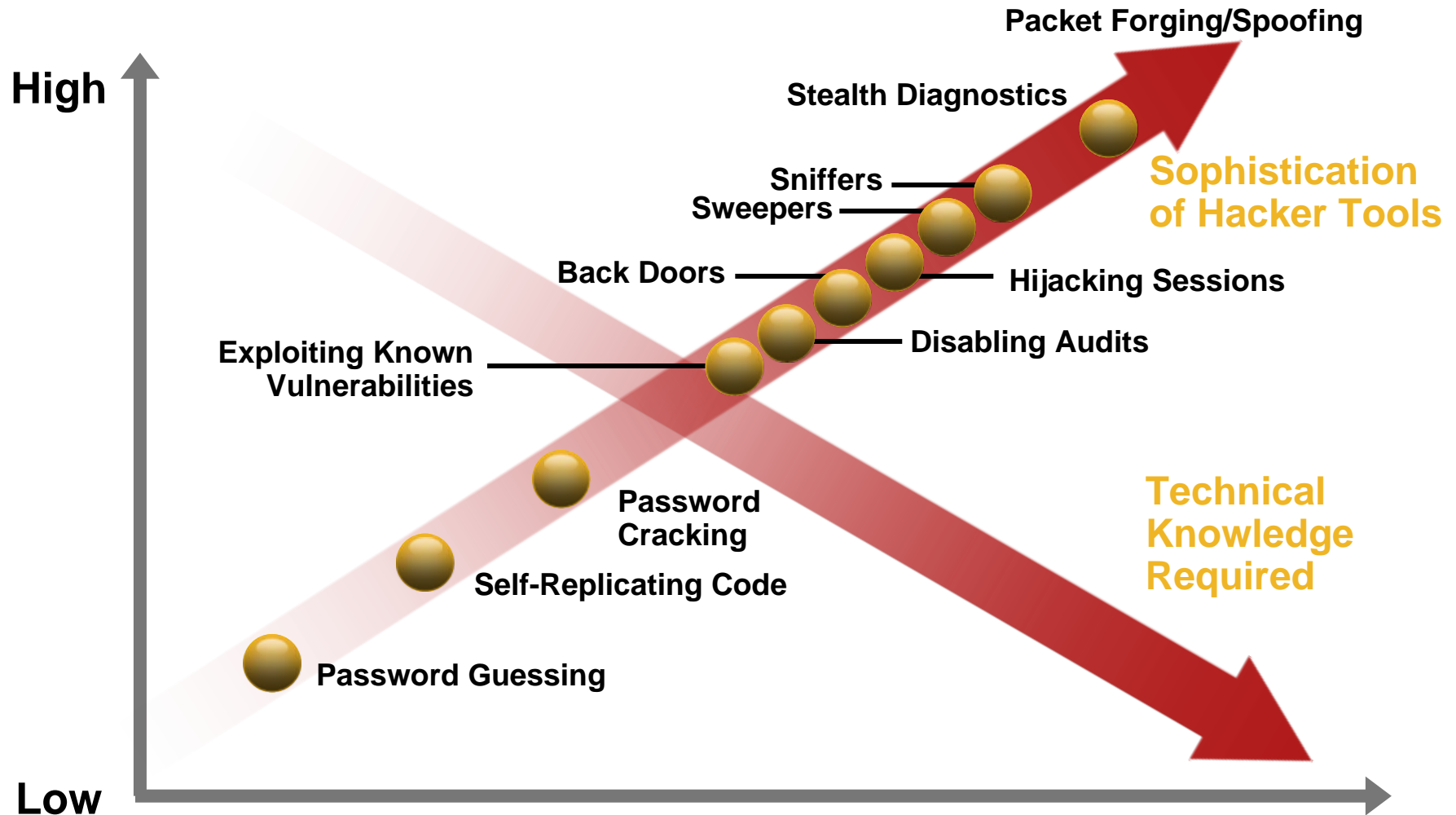
Version 13, Q3, FY09

Produced by the Cisco on Cisco team within Cisco IT

Threat Evolution



How Are the Threats Evolving?



Economics of Cyber Attacks

Have Dealt with So Far:

- Adolescents or effectively adolescents
- Operating alone or with one or two friends
- Primarily interested in causing entertaining mischief
- Heavily biased toward instant gratification
- Lacking in business expertise
- Operating only as remote intruders

Need to Worry About:

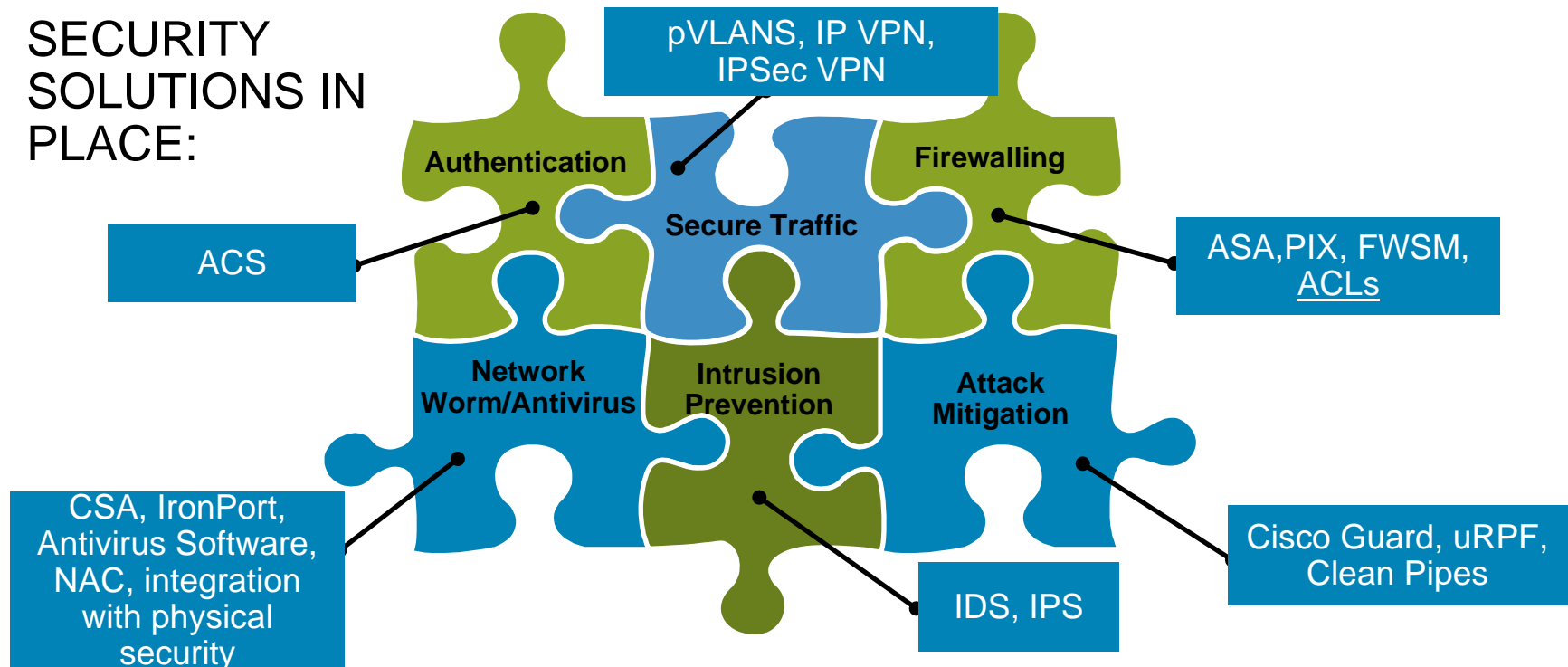
- Adults
- Supported by larger organizations with sizeable budgets
- Interested in inflicting maximum economic damage
- Willing to aim for delayed, initially invisible, long-term effects
- Well supplied with business expertise
- Operating sometimes with the assistance of insider agents

Self-Defending Network at Cisco

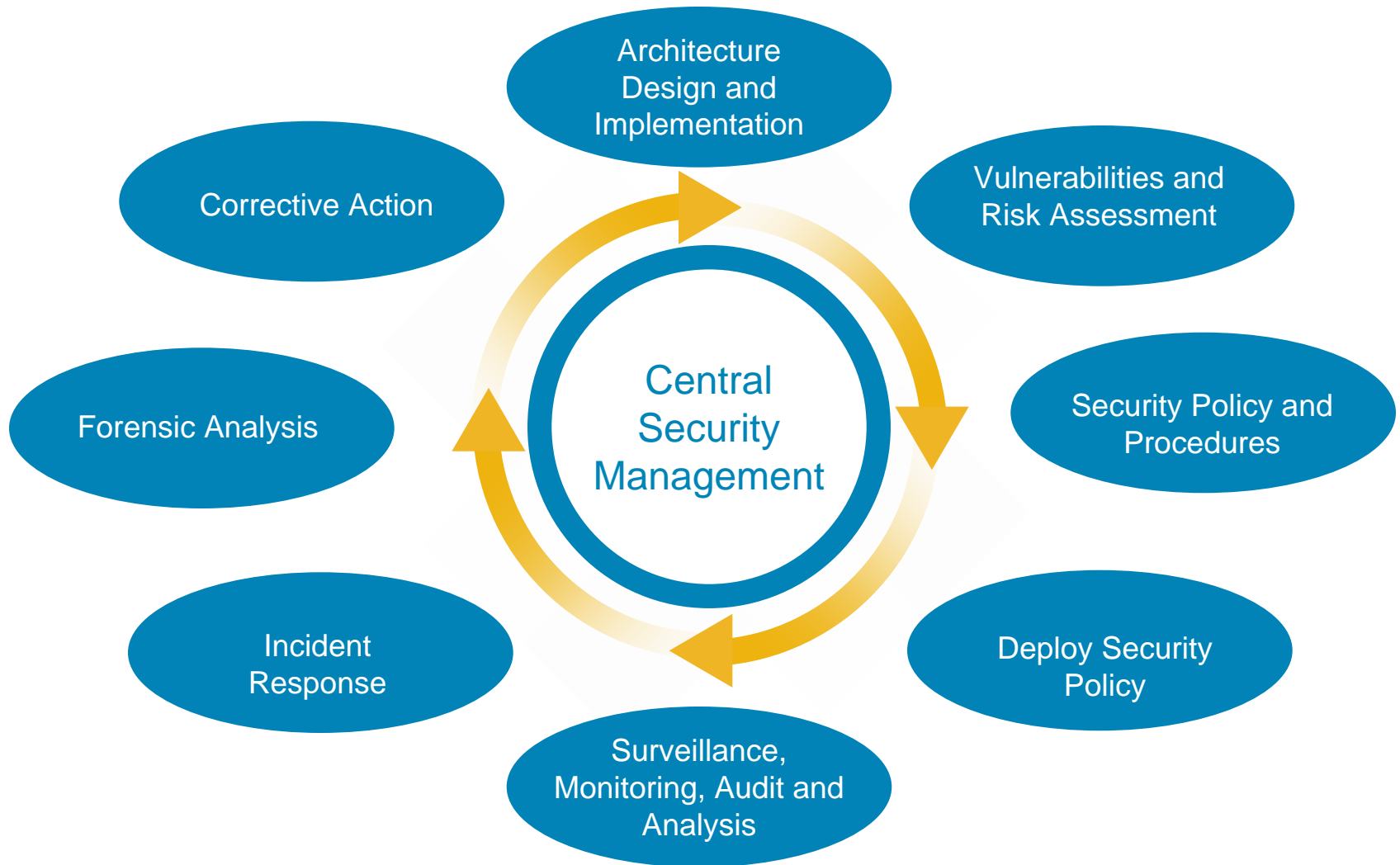
- Secure access; globally
Onsite, remote site, mobile worker, telecommuter
- Multiple layers of defense
Desktop, network, data center, application



SECURITY SOLUTIONS IN PLACE:



Security Is a Systematic Process



Executive Summary

Security



- Internet technology is critical to Cisco business:
- E-commerce (93% of orders by Cisco.com)
- Extended enterprise
- Remote access (1 in 4 employees work remotely and connect via Internet)



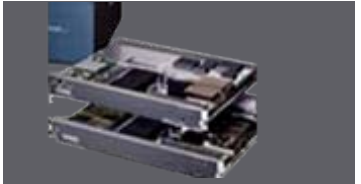
- Opening your business processes to the Internet brings with it an ever-increasing risk



- Regulations now require risk mitigation



- Network defense is changing from passive and reactive to active and proactive



- Cisco multilayer security solution in place supporting a self-defending network

Security – Move to a Proactive Model

Reactive

- Basic firewall (access control lists)
- Wireless static WEP
- IDS engines without data correlation or usage
- ACS on Solaris

Active

- Basic and advanced firewall (ACLs + FWSM)
- Wireless TKIP & MIC
- IDS appliances
- Cisco Security Agents on desktops
- Teleworker security policies
- DDoS mitigation
- Anomaly detection
- ACS on Solaris and Windows

Proactive

- Threat defense system:
 - Data correlation via SIMS
 - Wireless security 802.11i
 - IDS → IPS transition
 - Cisco Security Agent additions on Linux/Windows 2003 server
- Secure connectivity system
- Trust and identity management system
- Network Admission Control (NAC)

Security – Business Value Snapshot

Productivity

- Seamless, transparent solution minimizes business disruption



Quality/End User Experience

- Less time fighting and fixing attacks, reducing business disruption and damages



To learn more about real-world
Cisco IT deployments, visit
www.cisco.com/go/ciscoit

