expertise in action®

ACS®

Security in an Outsourced World

Presented by Christopher Leach, SVP, CISO

© Affiliated Computer Services, Inc. (ACS) 2009

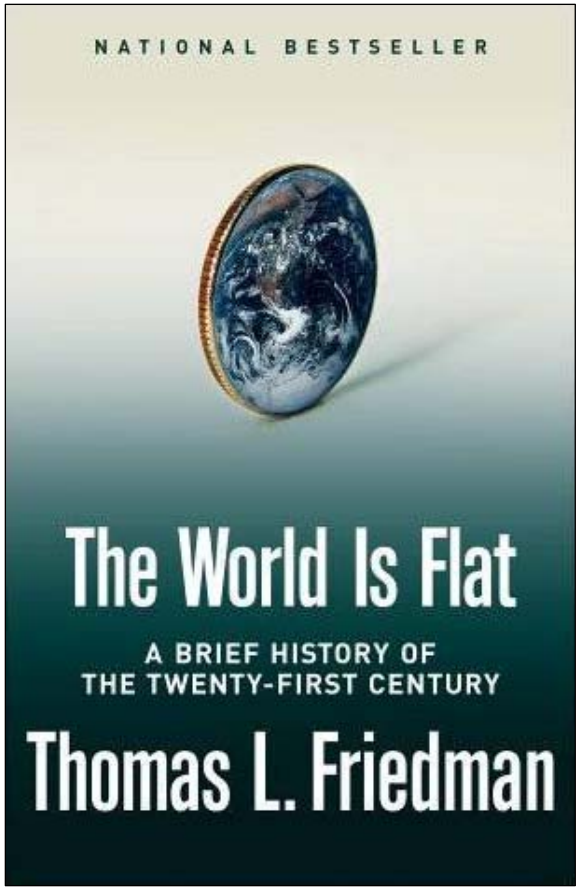
Learning Objectives

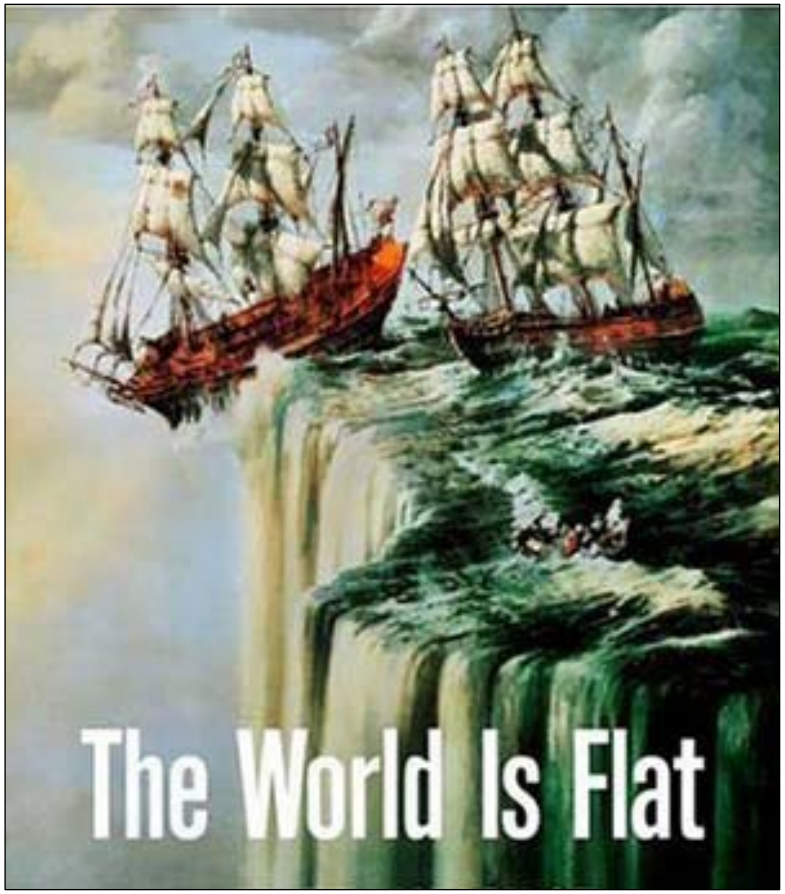
- Considerations when monitoring and maintenance of applications occurs in another country
- Security practices to look for in outsourced arrangements
- SAS 70 Type II control objectives to review
- Issues that can be exacerbated by rushing to outsource IT

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Ten Forces That Flattened the World





expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

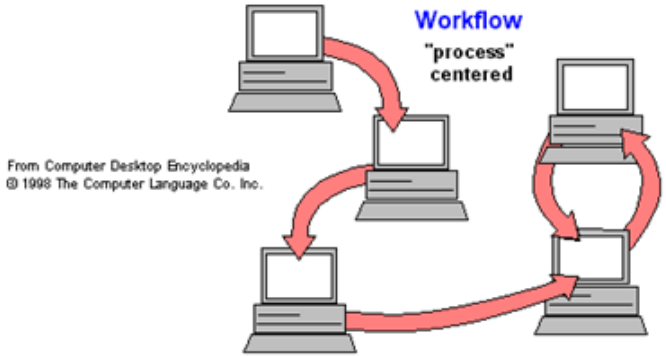
Ten Forces That Flattened the World

1 PC Revolution

2 Connectivity

3 Uploading

4 Outsourcing



5 Workflow Software

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Ten Forces That Flattened the World

6 Offshoring

7 Supply Chain

8 Insourcing

9 In-forming

10 Digital Devices

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Information Security Landscape

Mobile Technology Trends

•Data is walking out the door - Laptops, USB Drives, PDAs
•Malware and spyware for everyone

Mobile Workforce

•Always remote employees
•Flexible definition of the office
•Intranet access from customer sites

Network Reperimeterization

•Traditional perimeter security is not sufficient alone
•Emergence of new technology enablers

Global Outsourcing

•Others may manage your network
•Augmenting traditional IT – Software plus services (SaaS) remote data and applications
•Complex granular partner access controls

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Who Is Behind Data Breaches?

74% Resulted from external sources

20% Were caused by insiders

32% Implicated business partners

39% Involved multiple parties

Source: Verizon Business 2009 Data Breach Investigations Report

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

How Do Breaches Occur?

67% Were aided by significant errors

64% Resulted by hacking

22% Utilized malware

22% Involved privilege misuse

9% Occurred via physical attacks

Source: Verizon Business 2009 Data Breach Investigations Report

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

What Commonalities Exist?

69% Were discovered by a third party

81% Victims were NOT PCI compliant

83% Attacks were NOT highly technical/difficult

87% Were considered avoidable through simple/intermediate controls

99.9% Records compromised from servers or applications

Source: Verizon Business 2009 Data Breach Investigations Report

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Where Should Efforts Be Focused?

- Policy and procedures
- Risk/threat assessments
- Ensure controls are met
- Find, track and assess data
- Collect & monitor event logs
- Audit user accounts and credentials
- Test and review applications

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Vendor Selection Criteria

- Experience and expertise
- Supplier size, financial strength and culture
- Number of supplier competitors
- Legal/regulatory requirements
- What is being outsourced
  - Careful review of the contract
  - SLAs and other deliverables
- Where is the work being outsourced
  - Global privacy requirements
  - Global hotspots

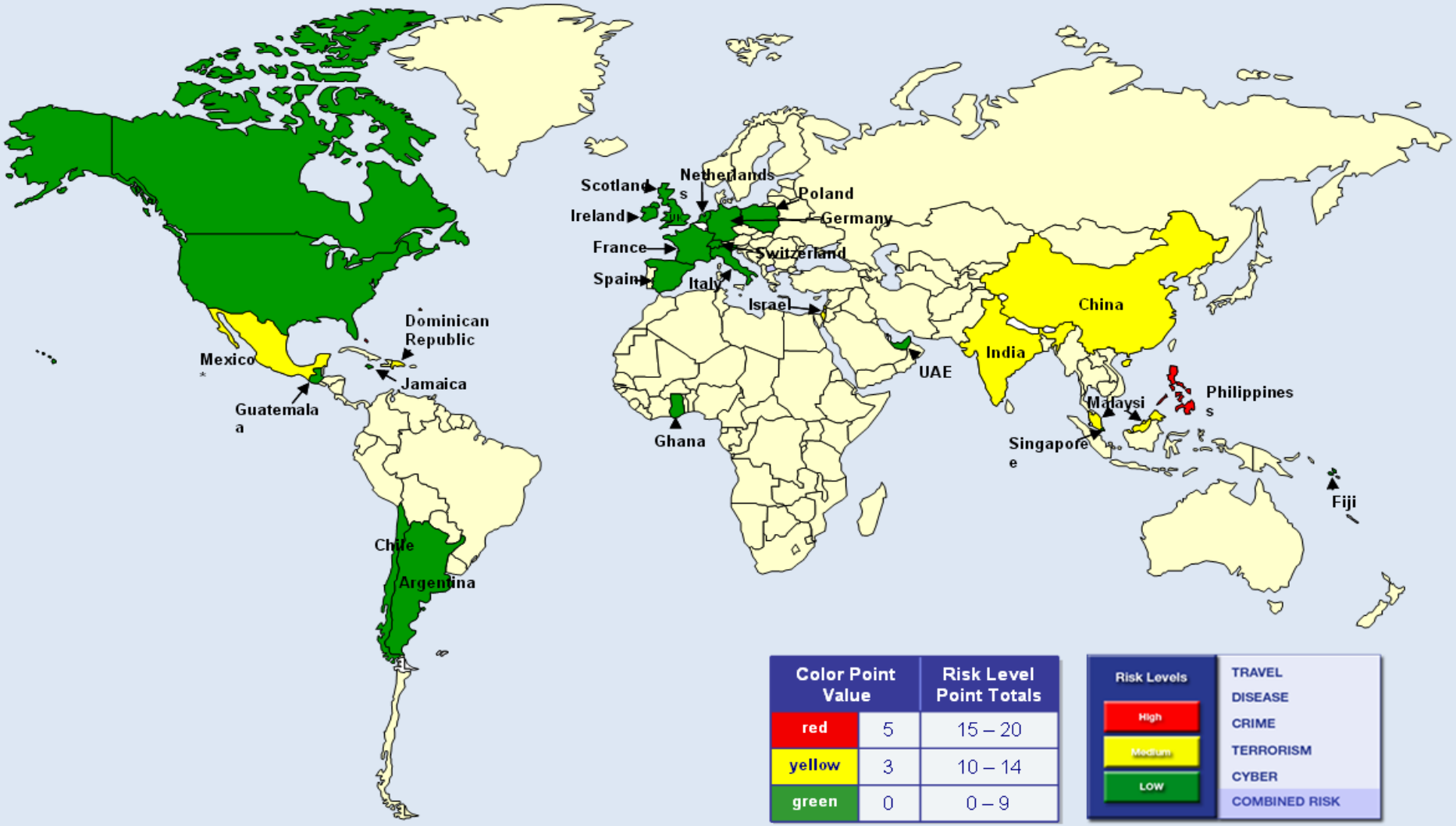
expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

ACS GLOBAL LOCATIONS

RISK / THREAT AREAS - COMBINED RISK

expertise in action™



Color Point Value		Risk Level Point Totals
red	5	15 – 20
yellow	3	10 – 14
green	0	0 – 9

Risk Levels	
High	TRAVEL
Medium	DISEASE
LOW	CRIME
	TERRORISM
	CYBER
	COMBINED RISK

Elements of a Good Security Program

Reporting accountability

- To whom does the CISO report?
- How often are reports created, reviewed and discussed?
- Are metrics monitored?
- Are improvements part of the management plan?

Strong Policies

- Reviewed on a routine basis
- Follow a prescribed standard (ISO, etc)
- Have business input

Leverages both technology and process controls

Has an awareness program

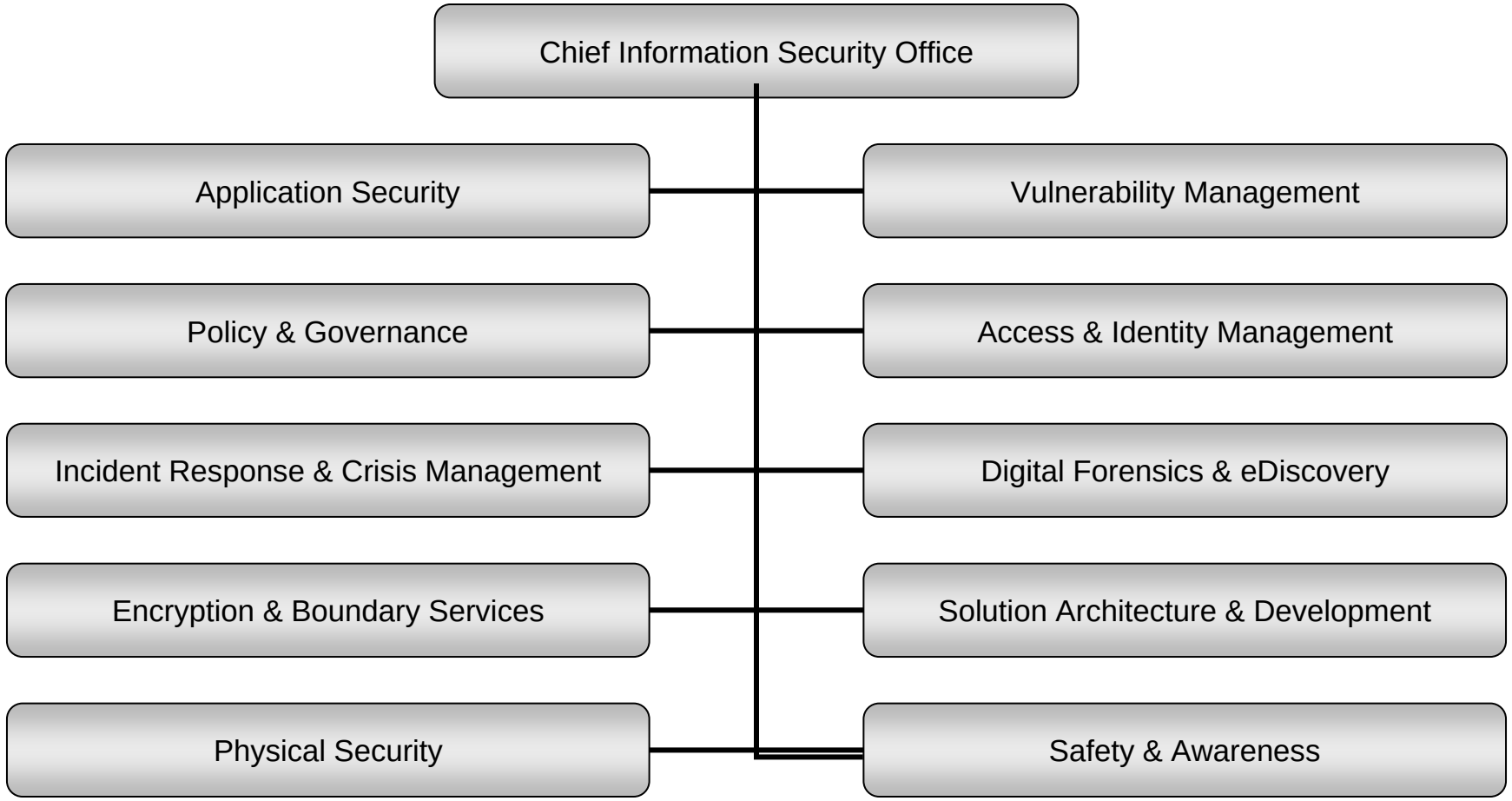
Considers physical components

Has an incident response or CIRT program

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

CISO Functional Structure



expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

A few closing thoughts

- What about a SAS70?
  - All SAS70 reports are not equal
  - Should consider the control environment previously discussed
  - Should consider the service auditor
- What about other certifications?
  - ISO 27001
  - PCI
  - SysTrust

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009

Questions

expertise in action™

© Affiliated Computer Services, Inc. (ACS) 2009