Foundstone
Professional Services
A DIVISION OF McAFEE

» What's Next?

Hacks-In-Taiwan 2006 Keynote

Yen-Ming Chen
Senior Principal Consultant
Foundstone, A Division of McAfee

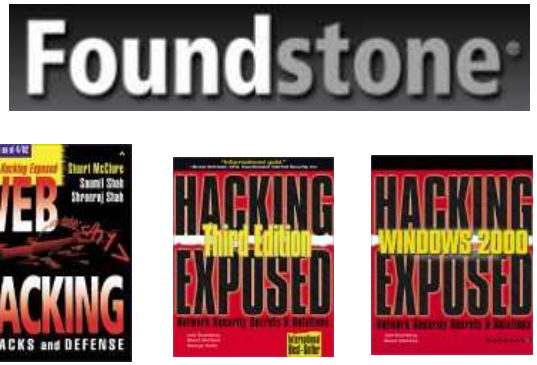
Agenda

- Introduction
- Security Ecosystem
- Security Trends
- Security Technology
- Conclusion

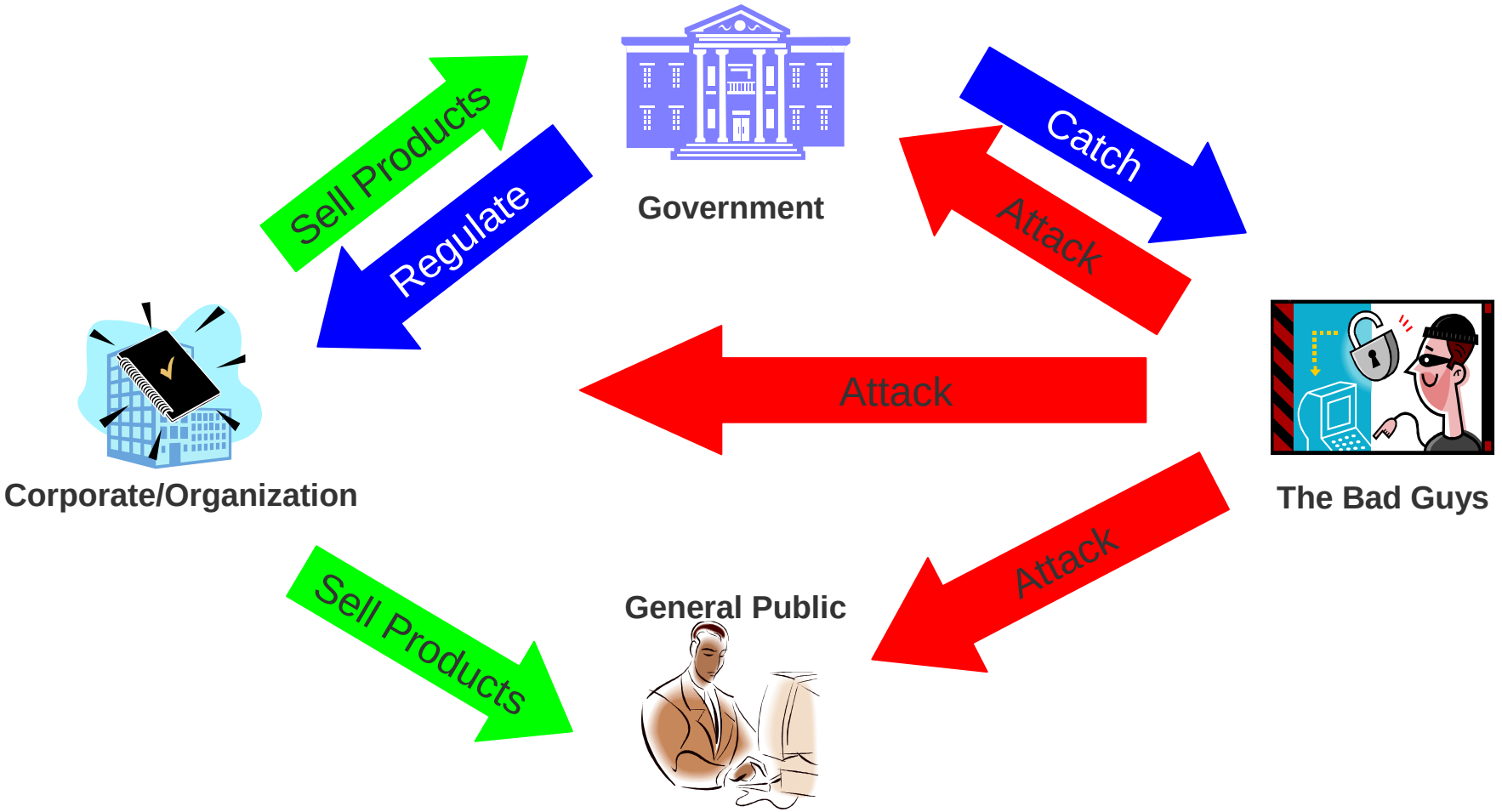
Introduction

Yen-Ming Chen

- Sr. Principal Consultant
- Been to 12 countries, 7 offices and 6 years with Foundstone
- Contributing author of four security books and numerous published articles.
- Master of Science in Information Networking from C.M.U.
- Provide security risk assessment from web applications to emerging technologies



Security EcoSystem



Foundstone
Professional Services
A DIVISION OF McAFEE

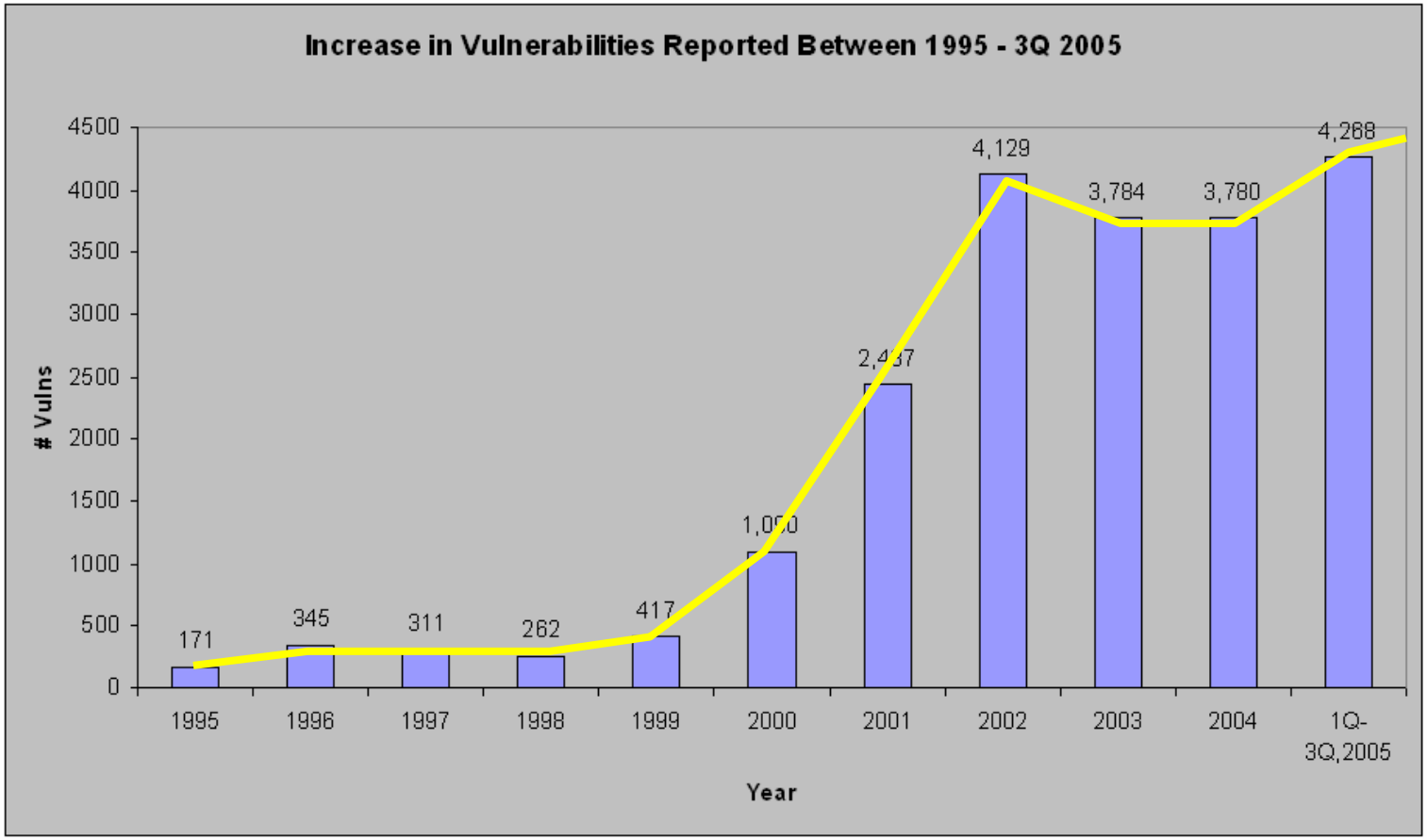
A Chronology of Data Breaches Reported Since the ChoicePoint Incident (Feb, 2005)

Unfortunately I am one of the innocent victim too!

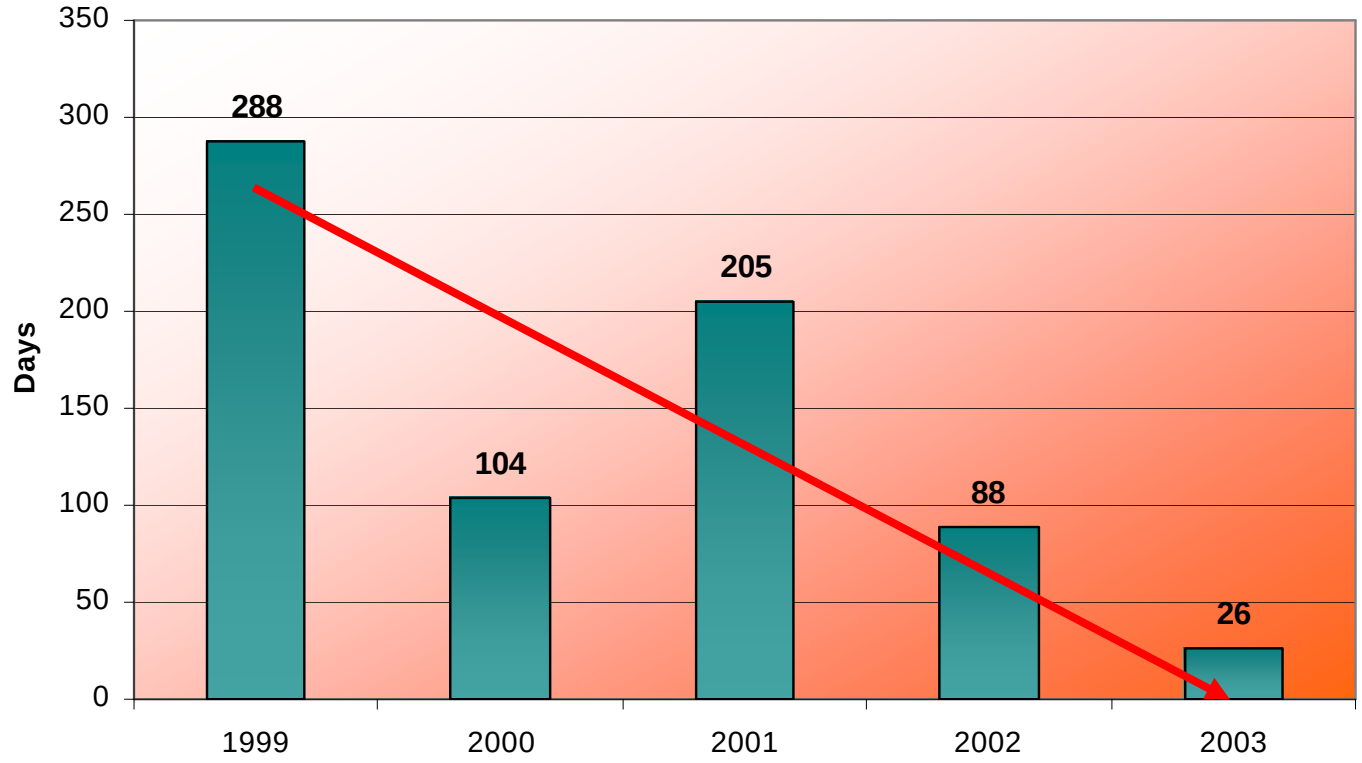
網址(D) http://www.privacyrights.org/ar/ChronDataBreaches.htm

2006	Tennessee (866) 748-1680	containing names, addresses and SSNs of about 36,000 past and current employees. Intruder apparently used computer from Aug. '05 to May '06 to store and transmit movies.	
July 7, 2006	Nat'l Association of Securities Dealers (NASD) (Boca Raton, FL)	Ten laptops were stolen on Feb. 25 '06 from NASD investigators. They included SSNs of securities dealers who were the subject of investigations involving possible misconduct. Inactive account numbers of about 1,000 consumers were also contained on laptops.	73
July 7, 2006	Naval Safety Center	SSNs and other personal information of naval and Marine Corps aviators and air crew, both active and reserve, were exposed on Center web site and on 1,100 computer discs mailed to naval commands.	"more than 100,000"
July 7, 2006	Montana Public Health and Human Services Dept. (Helena, MT)	A state government computer was stolen from the office of a drug dependency program. during a 4th of July break-in. It was not known if sensitive information such as SSNs was compromised.	Unknown
July 13, 2006	Moraine Park Technical College (Beaver Dam, Fond du Lac, & West Bend, WI)	Computer disk (CD) with personal information of 1,500 students was reported missing. Information includes names, addresses, phone numbers & SSNs of apprenticeship students back to 1993.	1,500
TOTAL number of records containing sensitive personal information involved in security breaches			**88,967,592**

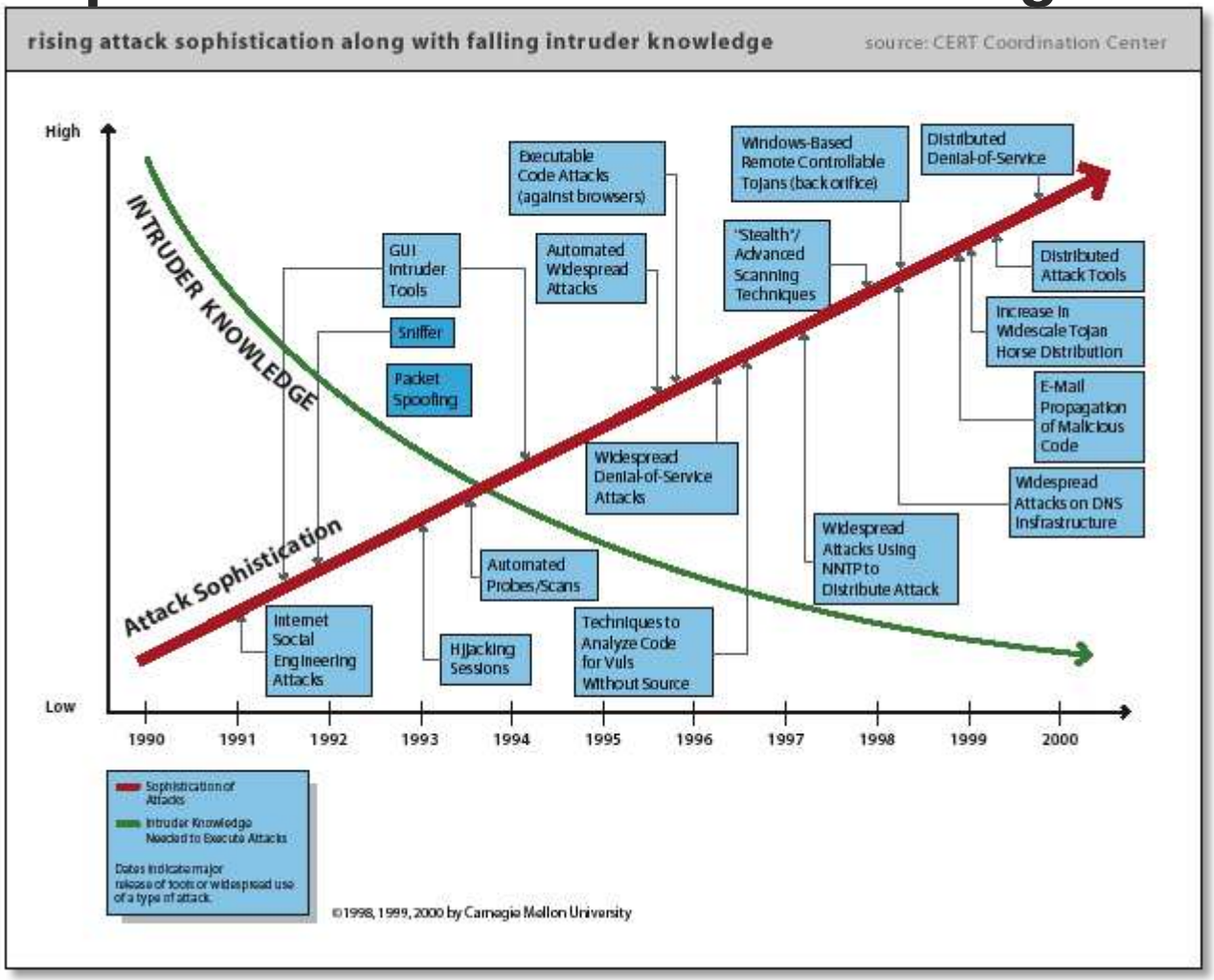
Security Trend – The Problem



Vulnerability-to-worm cycle is shrinking…



The sophistication of attacks is rising…



Internet security has come a long way…

- Internet “Darwinism” = Survival of the Fittest
- From Reactive to Proactive
- From Assessing to Managing

- Firewalls
- Antivirus

- Intrusion detection
- Vulnerability assessment

- Consolidate authorization
- Outsourcing grunt work

- Application security
- Security resource dashboard

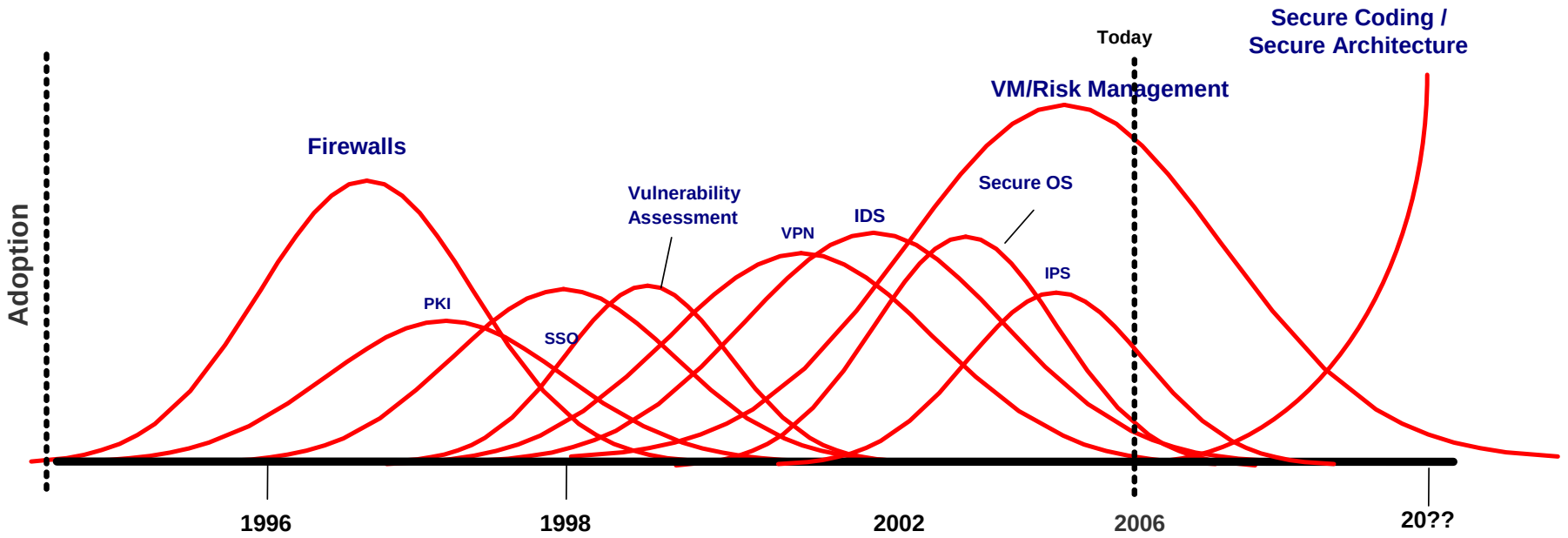
- **Enterprise Vulnerability Management Systems**
- Risk Management Dashboard





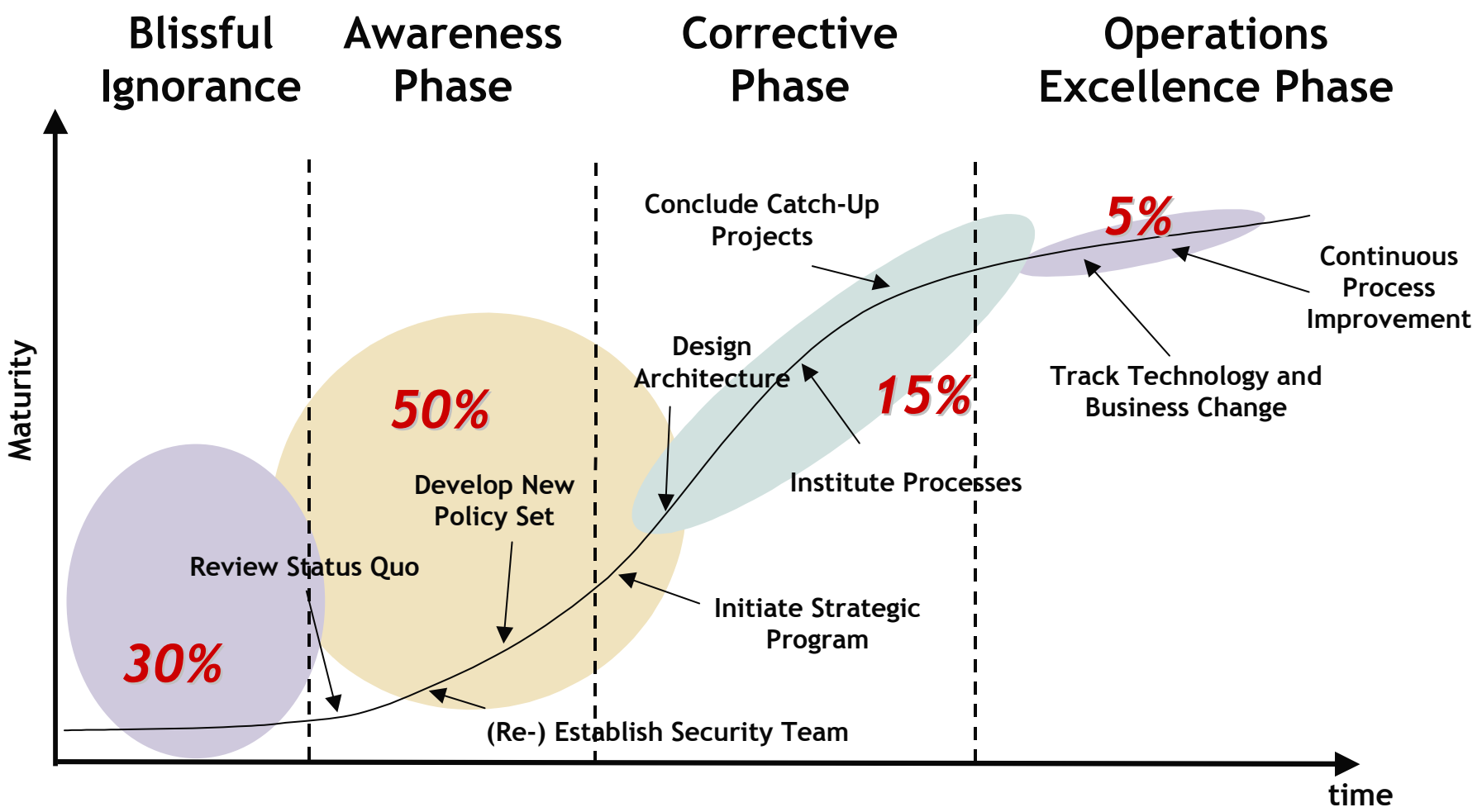
Gartner “Managing the Risks of IT Security” September 2002

Security Technology



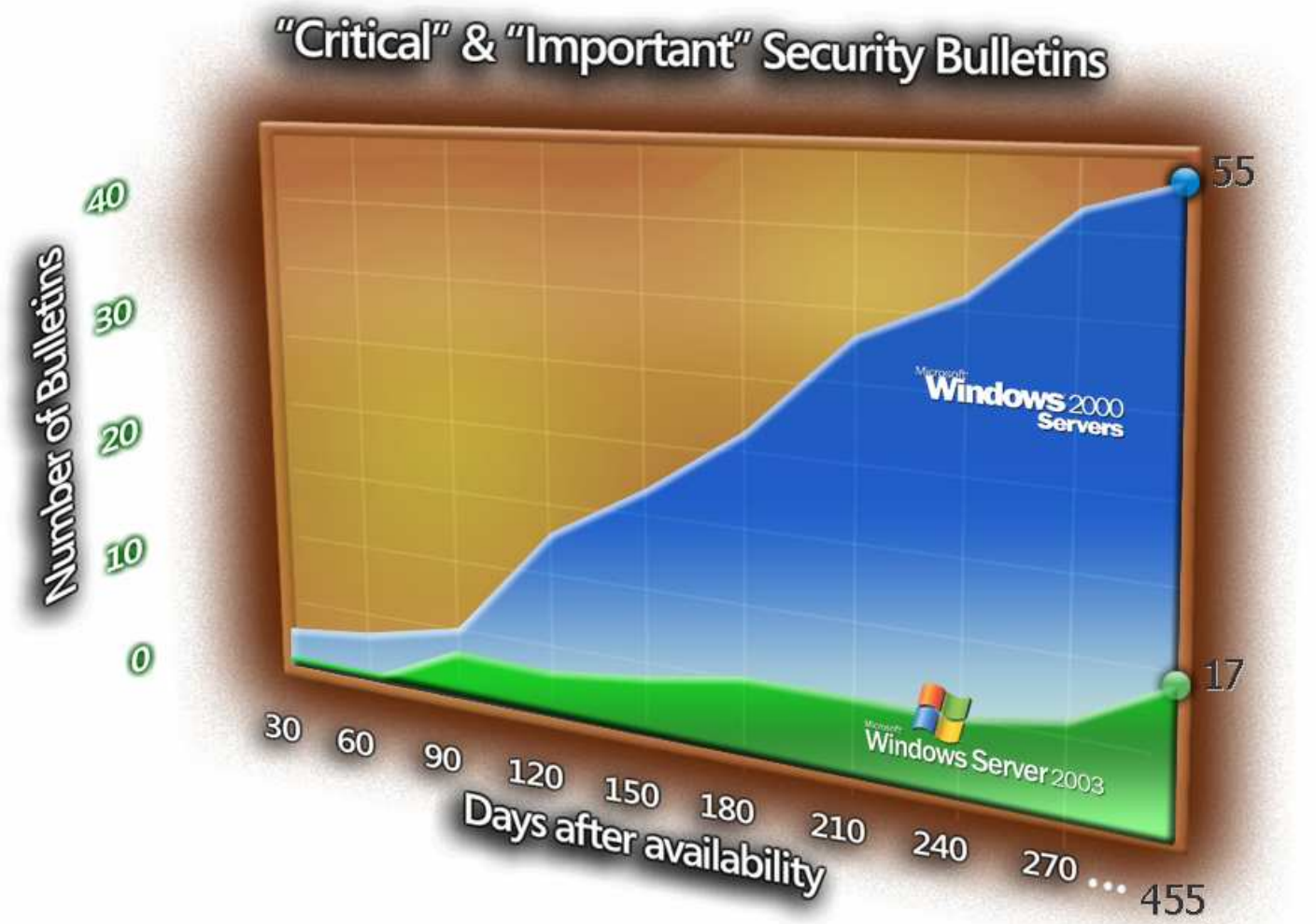
Foundstone Professional Services
A DIVISION OF McAFEE

Information Security Maturity: 2004



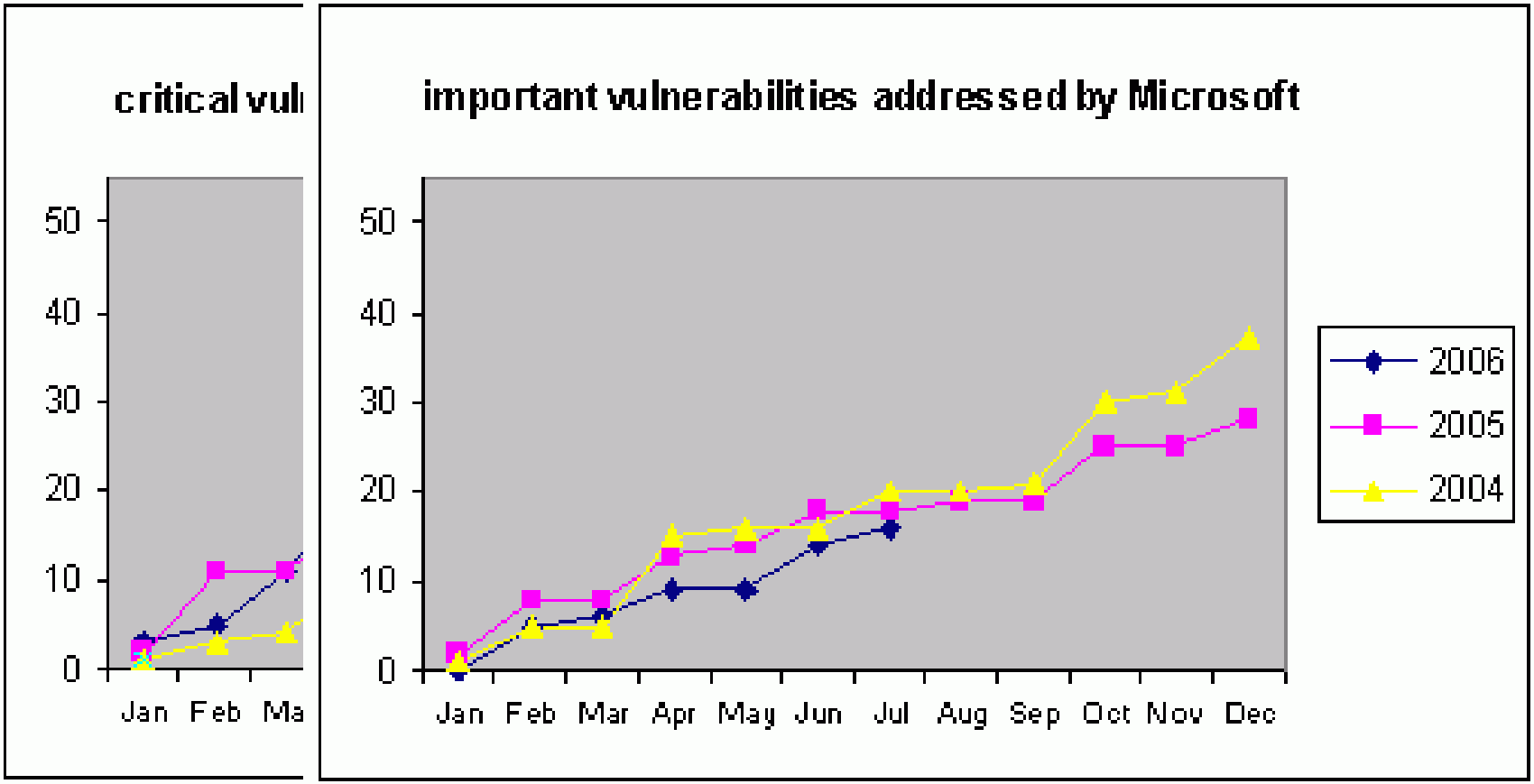
NOTE: Population distributions represent typical, large G2000-type organizations

Microsoft's Software Security Enlightenment



http://www.acsac.org/2004/dist.html

Here is another perspective



Source: http://www.avertlabs.com/research/blog/?p=53

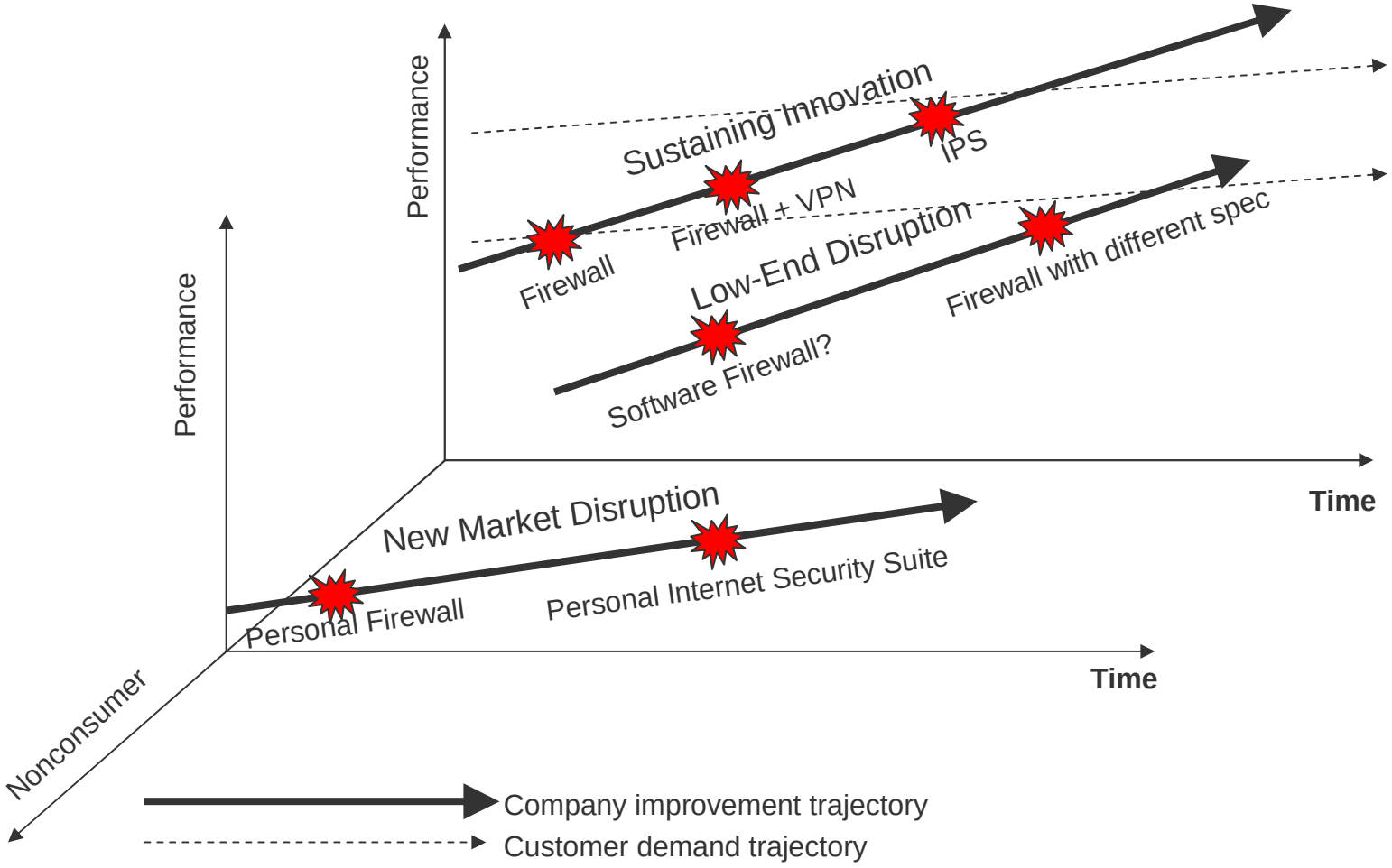
In fact, almost every security technology depends on vulnerabilities…

Technology	Role in vulnerabilities?
Anti-virus	*Vulnerabilities* in software, end-user usage.
Firewalls/VPN	Blocking attackers taking advantage of *vulnerabilities*
Identity Mgmt	*Vulnerability* inherent in online identities.
NIDS/HIDS	Detecting hackers exploiting *vulnerabilities*
NIPS/HIPS	Detecting and preventing hackers exploiting *vulnerabilities*
Event Correlation	Addressing the data overflow issue caused by *vulnerabilities*
Policy Management	Ensuring compliance to prevent attacks on *vulnerabilities*
Authentication/Authorization	Hackers taking advantage of *vulnerable* passwords, few controls
Encryption	Hackers viewing *vulnerable*, cleartext files
Patch/Systems Mgmt	Fixing *vulnerabilities*
Vulnerability Mgmt	Discovering and managing *vulnerabilities*

Disruptive or Sustaining?

- Disruptive Innovation
  - Introducing new dimensions of performance compared to existing innovations
  - Creates new markets or offer more convenience or lower prices to customers
- Sustaining Innovation
  - Introducing improved performance compared to existing products and services

Firewall as an Example



What's Next?

- Security Integration
  - Make security as part of your business
  - Make security as part of your daily operation
  - Make security as part of your life
- Fundamental problems:
  - Trust
  - Balance

Security Integration

- Events happening in the industry:
  - Corporate M&A
    - 3Com/Cisco buying security companies
    - Symantec + Veritas
    - EMC + RSA
  - Company expands into security
    - Microsoft
      - SDL, Anti-Virus, integrate security into SMS and MOM
    - Verizon, Nortel and other service provider, telecoms
      - start providing security consulting services
- Security-only companies in the long run?
  - Attack competitor's credibility
  - 0-days to keep advantage

Security Integration – RPV Analysis

- Resource
  - Non-security companies have resources in
    - Product development skills
    - Cash
    - Channels and customers
- Process
  - Market research
  - Resource allocation
- Value
  - Provide security on top of existing product
    - Add-Value to existing customer
    - Easier to be accepted

Trust and Balance

- Abusing trust relationship
  - Attackers are shifting between targets
    - Network -> Server -> (Web) Application -> Browser
  - Researchers are seeking solutions
    - Firewall -> Vulnerability Scan -> Trusted Computing Platform -> SDL
- Balance
  - Password policies that don't make business sense
  - Unplug the network to keep it secure?!#$^
  - Security testing should be part of QA process

Conclusion

- Security will never die; But it won't be effective until fully integrated into business
  - Don't expect silver bullet or "easy button" because there is none!
  - Automation is a paradigm shift; Necessary evil; Hard problem too!
- Fundamental problems need to be solved
  - 'Trust' and 'Balance'
- Expand your horizon
  - Need to understand the technology, and innovation to know where you are going to next!

Foundstone
Professional Services
A DIVISION OF McAFEE

» Question & Answer

Thank You!

Yen-Ming Chen
ychen@foundstone.com