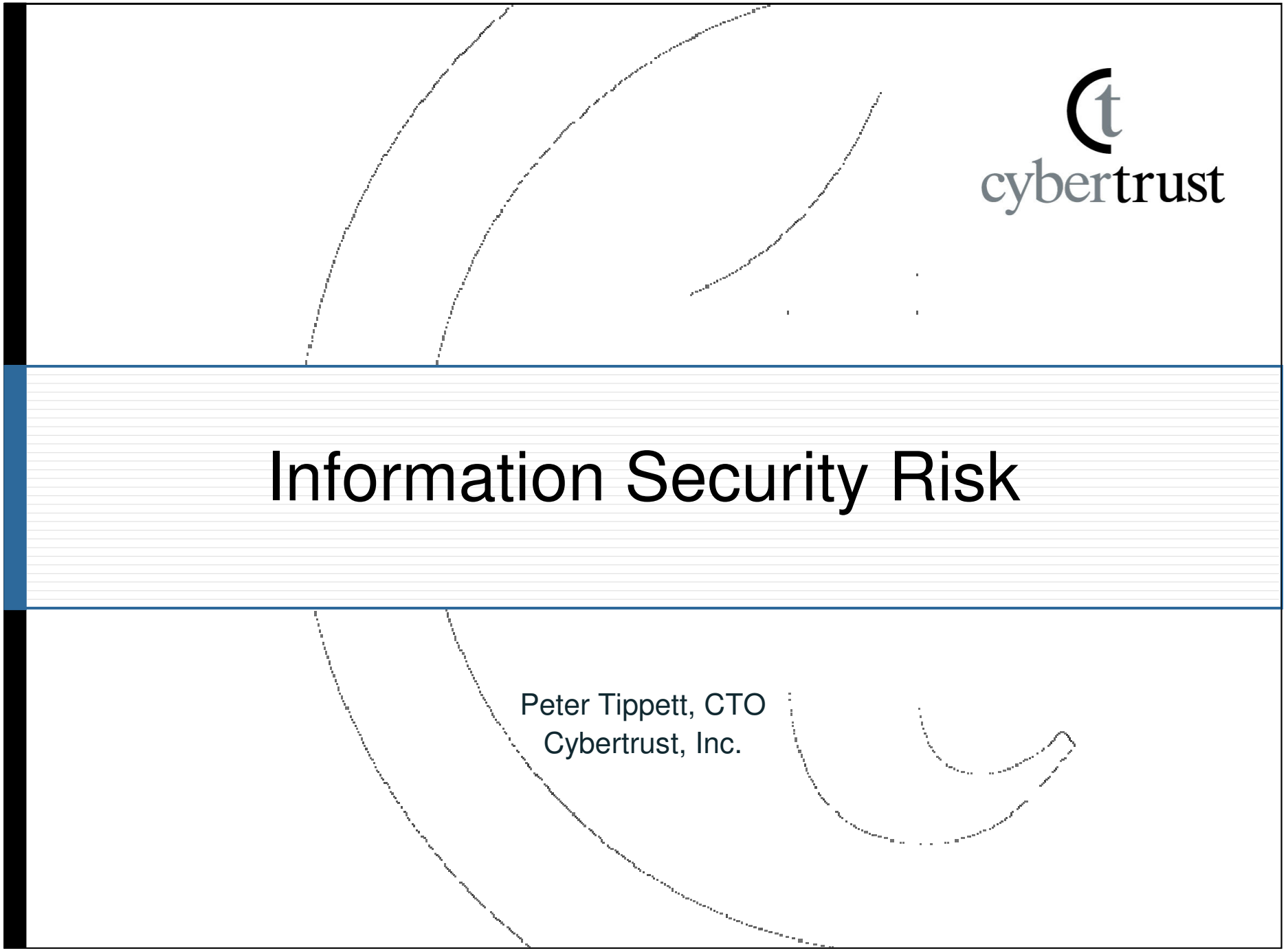


Information Security Risk

Peter Tippett, CTO
Cybertrust, Inc.

Who is Cybertrust ? Largest

Who can access what?

Control sources
PKI, ID, Passports…

Identity
Management

Betrusted
Providing Trust Worldwide

Top Tier Trust Services Provider-

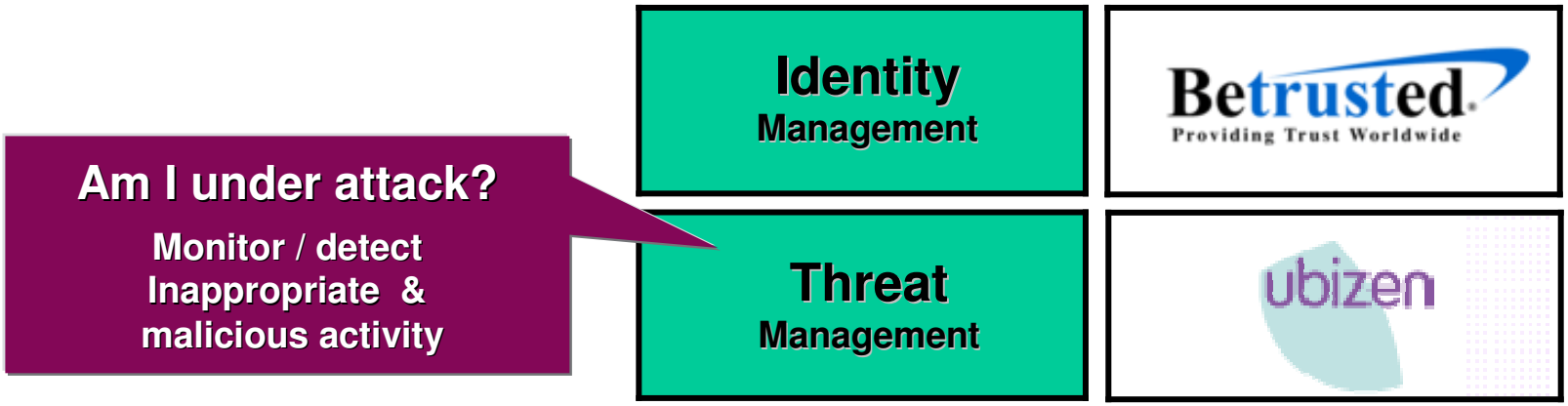
Leading provider of PKI solutions for governments and enterprises

Proven expertise in identity cards

Enterprise SSL and other credentials

Trillions of dollars dependent on Cybertrust Certificates every day

Who is Cybertrust ? 31 Offices World Wide

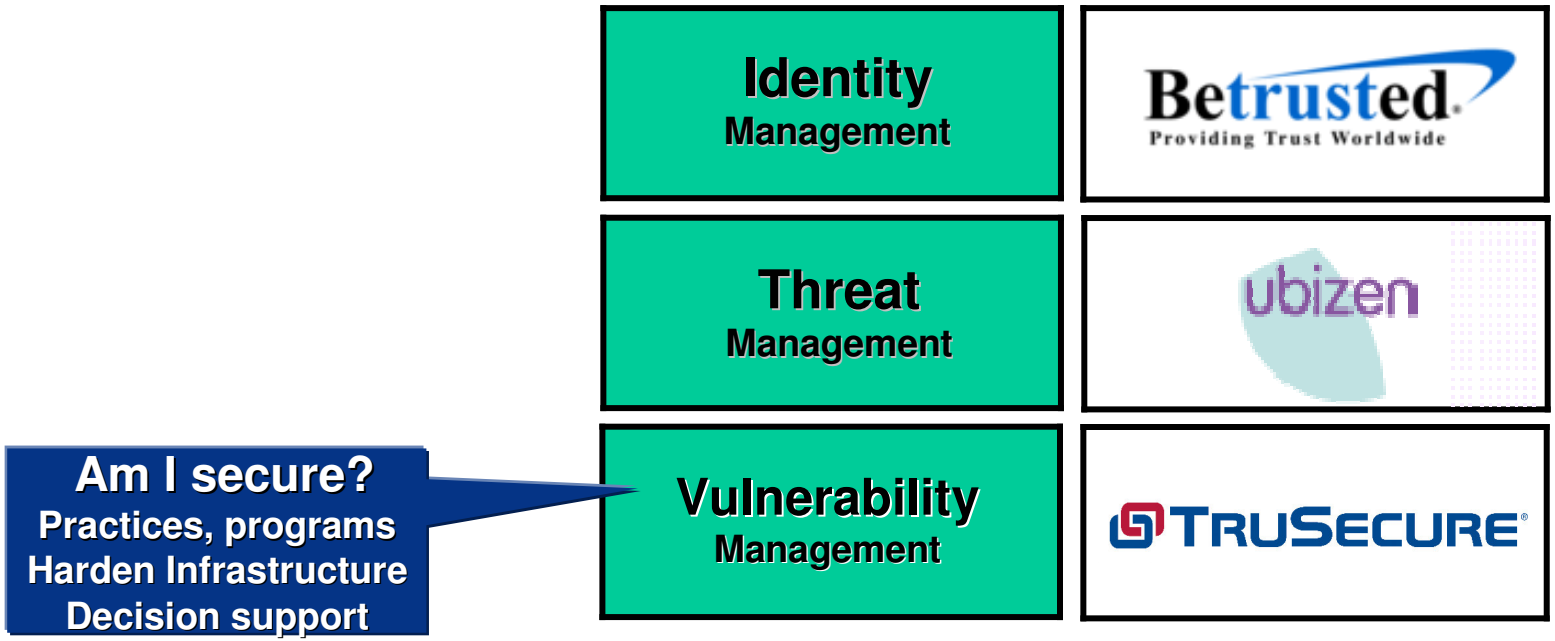


Largest Managed Security Services Provider –

Threat management to some of the largest companies in the world

Trust Centers Worldwide

Who is Cybertrust ? >1,000 Employees



Leading Security intelligence and analysis– 70+ people doing research, creating and distributing security intelligence and analysis daily to customers, product vendors and internally to drive products and services

Who is Cybertrust ?

Leading Security Risk Management and Compliance Programs, Process and Services pioneered to provide customers with the ability to predict, prioritize and adapt to real information security risks

Am I doing enough?
7799, SoX, GLB, VISA/MC Basel II, HIPAA, HSPD-12 etc.

Identity Management	Betrusted. Providing Trust Worldwide
Threat Management	ubizen
Vulnerability Management	TruSecure
Compliance Management	ALL

>4,000 Corporate Clients

Welcome

Who is Cybertrust?

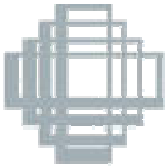
Top 5 Security Drivers / Predictions:

1. Actual Losses: Up each year
2. Cost of Security Up each year

Flat - Earth Thinking, Round- Earth World

Risk Models That Work

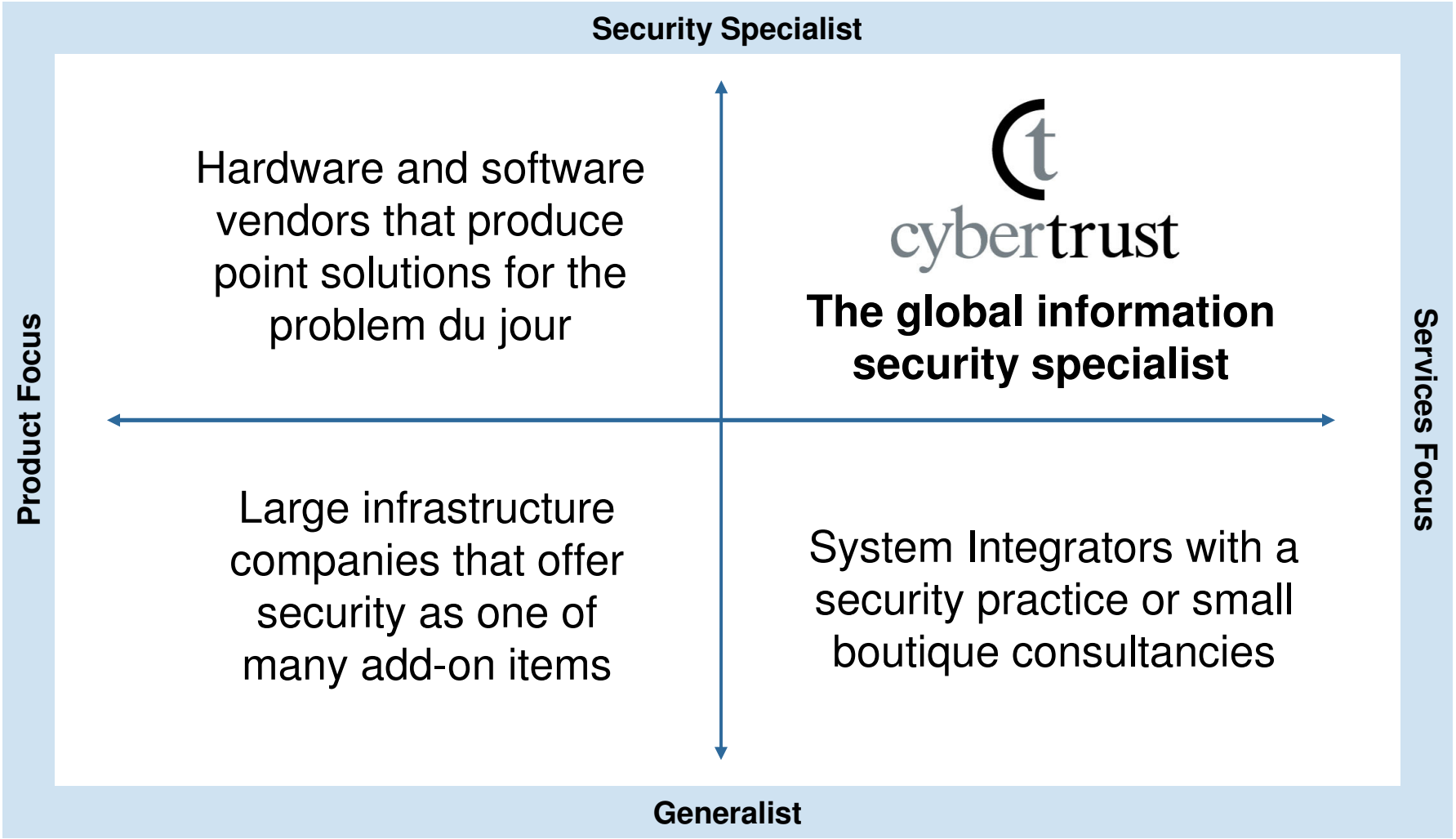
Who were you before Cybertrust ?



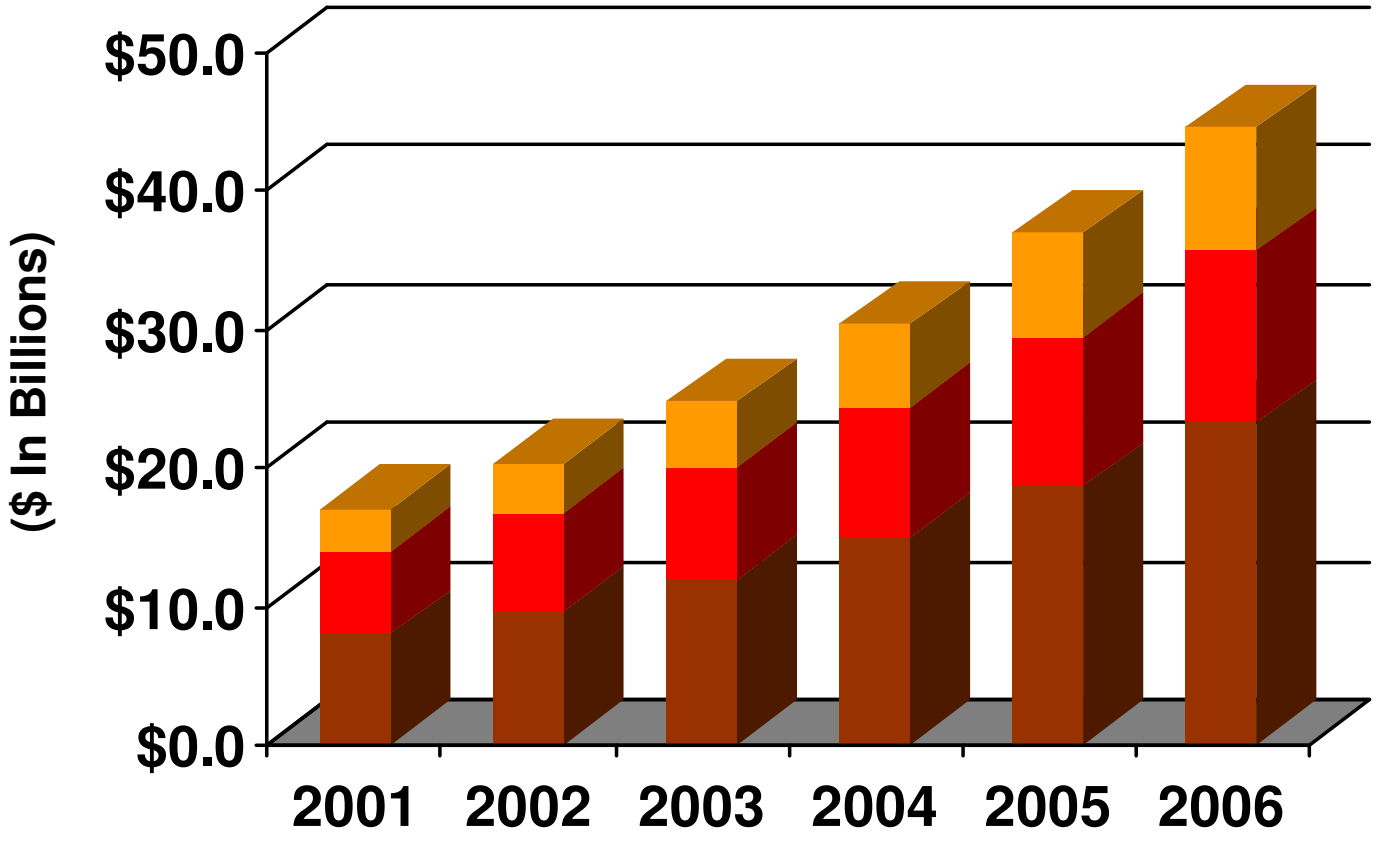
WildList Organization

firewall wizards

A Unique Business Profile (builds)



Security Spending



Source: IDC

Hacking - International Security Breaches - 2005

2/15 – ChoicePoint
2/25 – Bank of America
2/25 – PayMaxx
3/08 – DSW Shoes
3/10 – LexisNexis
3/11 – U CA Berkeley
3/11 – Boston College
3/12 – Nevada DMV
3/20 – Northwestern
3/20 – UNLV
3/22 – Cal State Chico
3/23 – U CA SF
4/04 – Georgia DMV
4/05 – MCI
4/08 – SJ Medical
4/11 – Tufts University
4/12 – Polo RalphLauren
4/14 – CA FasTrack
4/15 – CA Dept of Health
4/18 - DSW Shoes
4/20 – Ameritrade
4/21 – Carnegie Mellon
4/26 – Michigan State
4/26 – CSJ Hospital
4/28 – Georgia Southern
4/28 – Wachovia
4/29 – Oklahoma State
5/02 – Time Warner
5/04 – CO Dept of Health
5/05 – Purdue Univ
5/07 – DOJ
5/11 – Stanford Univ
5/12 – Hinsdale High
5/16 – Westborough Bank
5/18 – Jackson CC
5/19 – Valdosta State
5/22 – CardSystems
5/26 – Duke Univ
5/27 – Cleveland State
5/28 – Merlin Data Svcs
5/30 – Motorola
6/06 – Citi Financial
6/10 - FDIC
6/17 – Kent State
6/18 – U of Hawaii
6/22 – Eastman Kodak
6/25 – UCONN
6/29 – Bank of America
7/01 - UCSD
7/6 – City Natl Bank
7/7 – Michigan State
7/19 – USC
7/21 – Univ of Colorado
7/30 – San Diego Retirement
7/30 – Cal State
7/31 – Cal Poly
8/2 – Univ of Colorado
8/8 – Sonoma State
8/9 – Univ of Utah
8/10 – Univ North Texas
8/17 – Cal State
8/19 – Univ of Colorado
8/20 – US Air Force
8/27 – Unif of Florida
8/29 – JP Morgan

Identity Losses, Big Press, Real Issue
Government issue too

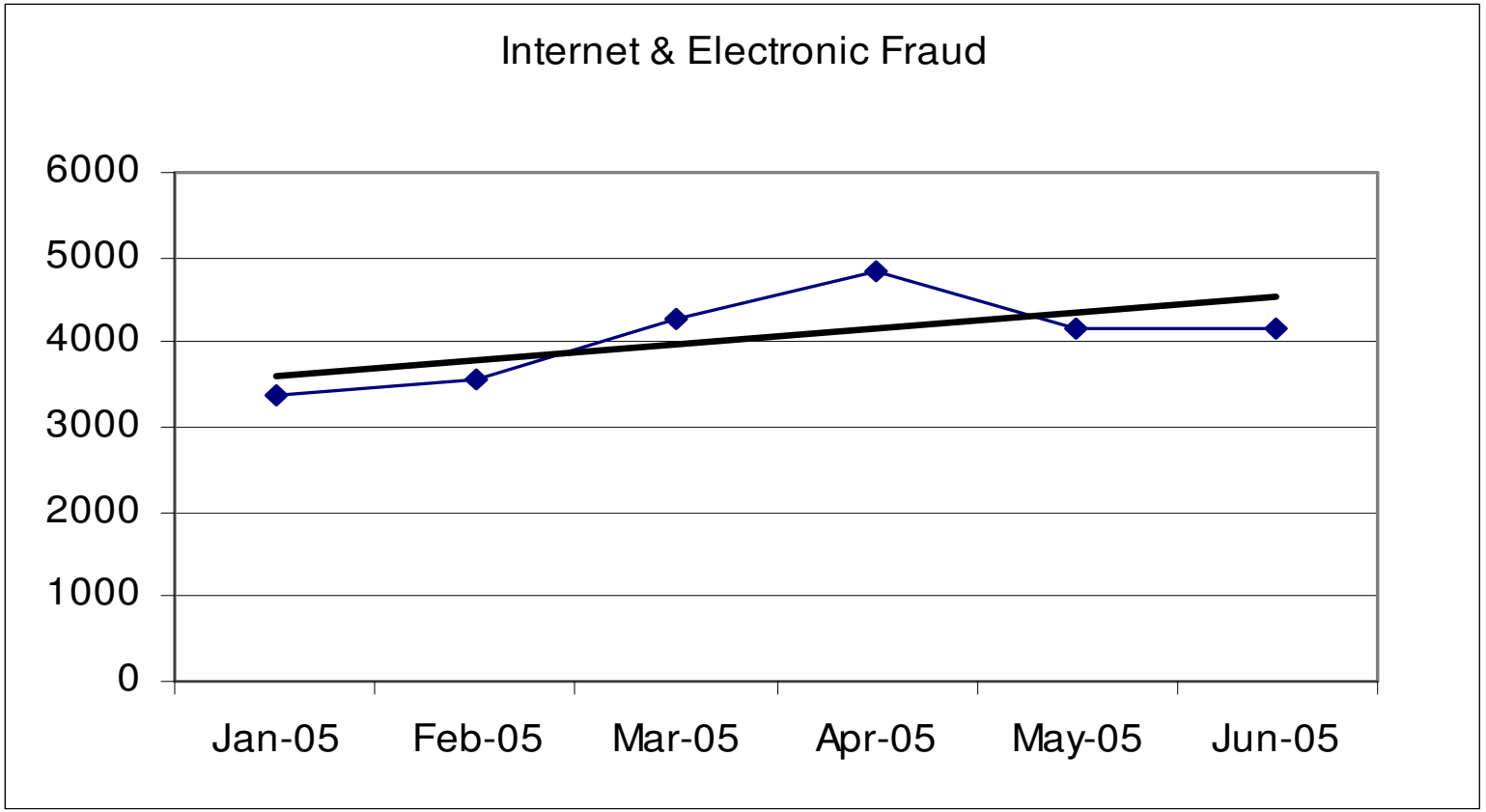
DATE ANNOUNCED TO THE MEDIA	COMPANY	TYPE OF BREACH	ACCOUNTS POTENTIALLY AFFECTED
Feb. 15	ChoicePoint	ID thieves accessed accounts	145,000
Feb. 25	Bank of America	Lost backup tape	1,200,000
March 9	LexisNexis	Passwords compromised	310,000*
April 18	DSW/Retail Ventures	Hacking	1,400,000
April 20	Ameritrade	Lost backup tape	200,000
April 28	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
May 2	Time Warner	Lost backup tape	600,000
June 6	CitiFinancial	Lost backup tape	3,900,000
June 18	CardSystems	Hacker	40,000,000

* The company initially announced that 32,000 accounts may have been breached, but increased the number to 310,000 in April.

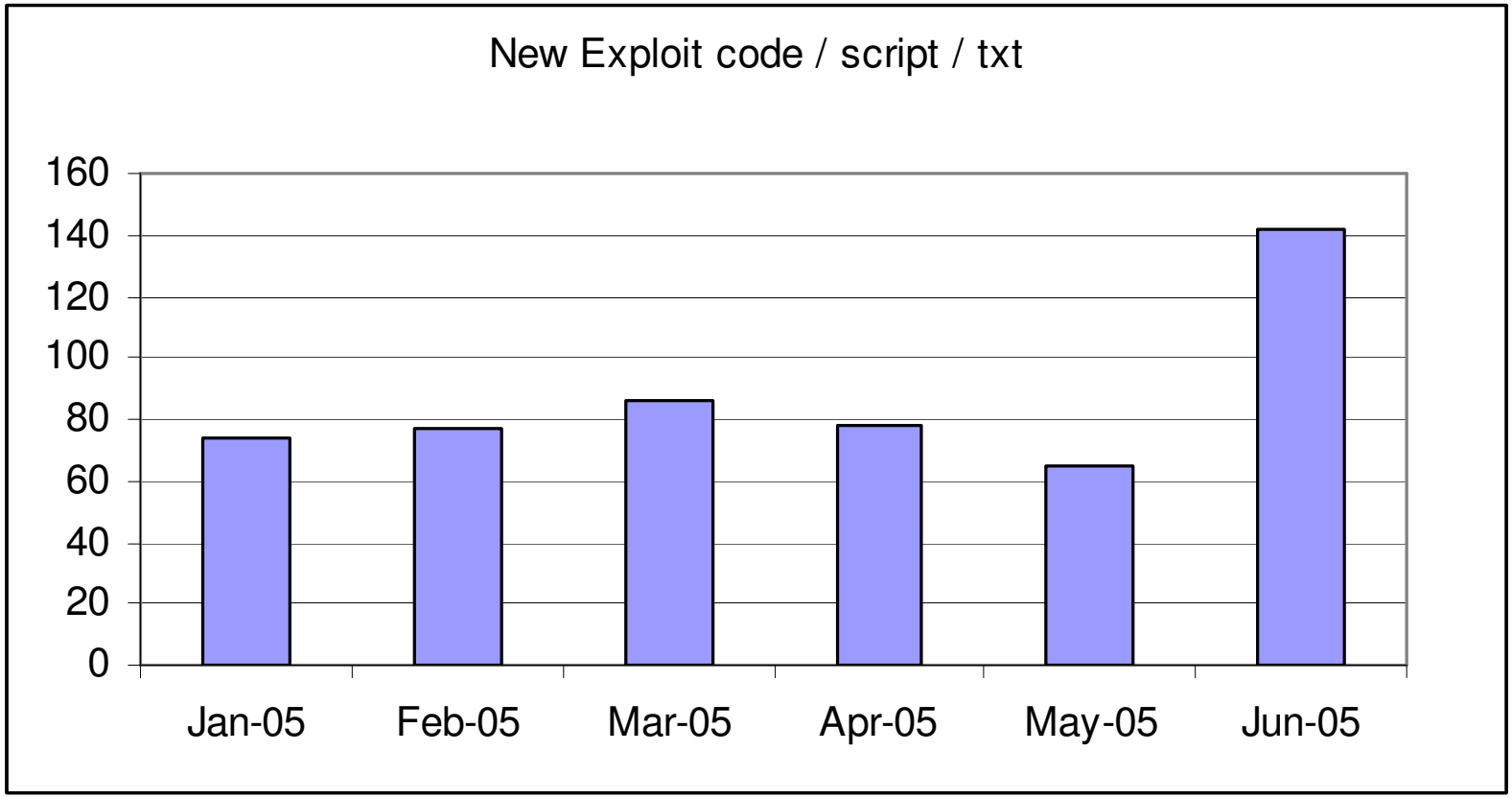
- On August 4, 2005, a California court ordered the credit-card payments processor Card Systems Solutions and three other defendants (MasterCard International, Merrick Bank and Visa USA) in a class action lawsuit…The breach exposed that CardSystems held information on 40 million credit-card accounts….**Visa and American Express have terminated their relationship with CardSystems** while MasterCard has stated it will review it's relationship with CardSystems
  Source: Gartner, August 2005

- **Visa / MC PCI Standard**
  Was CISP

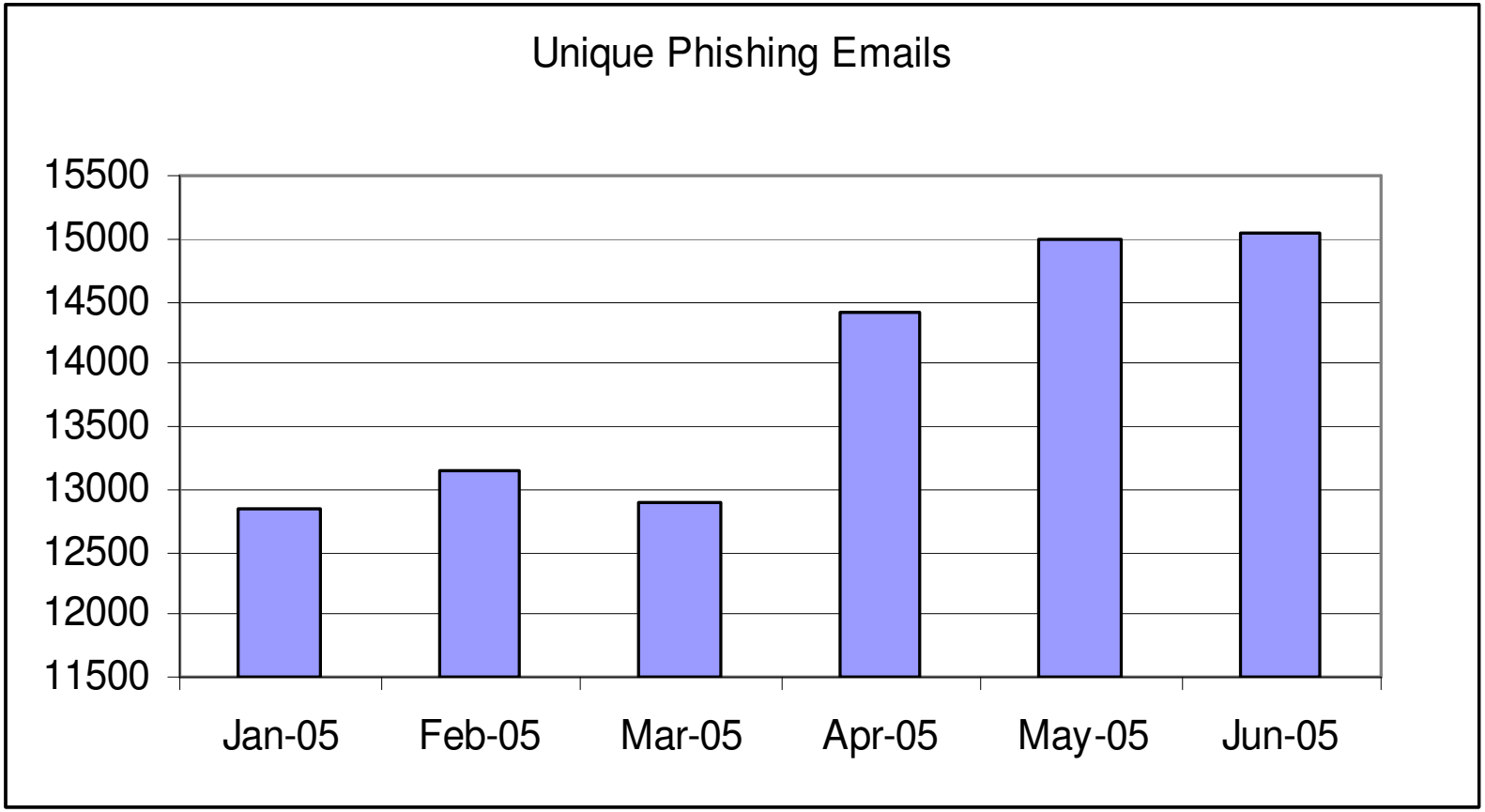
Threat Data
E-Fraud Index



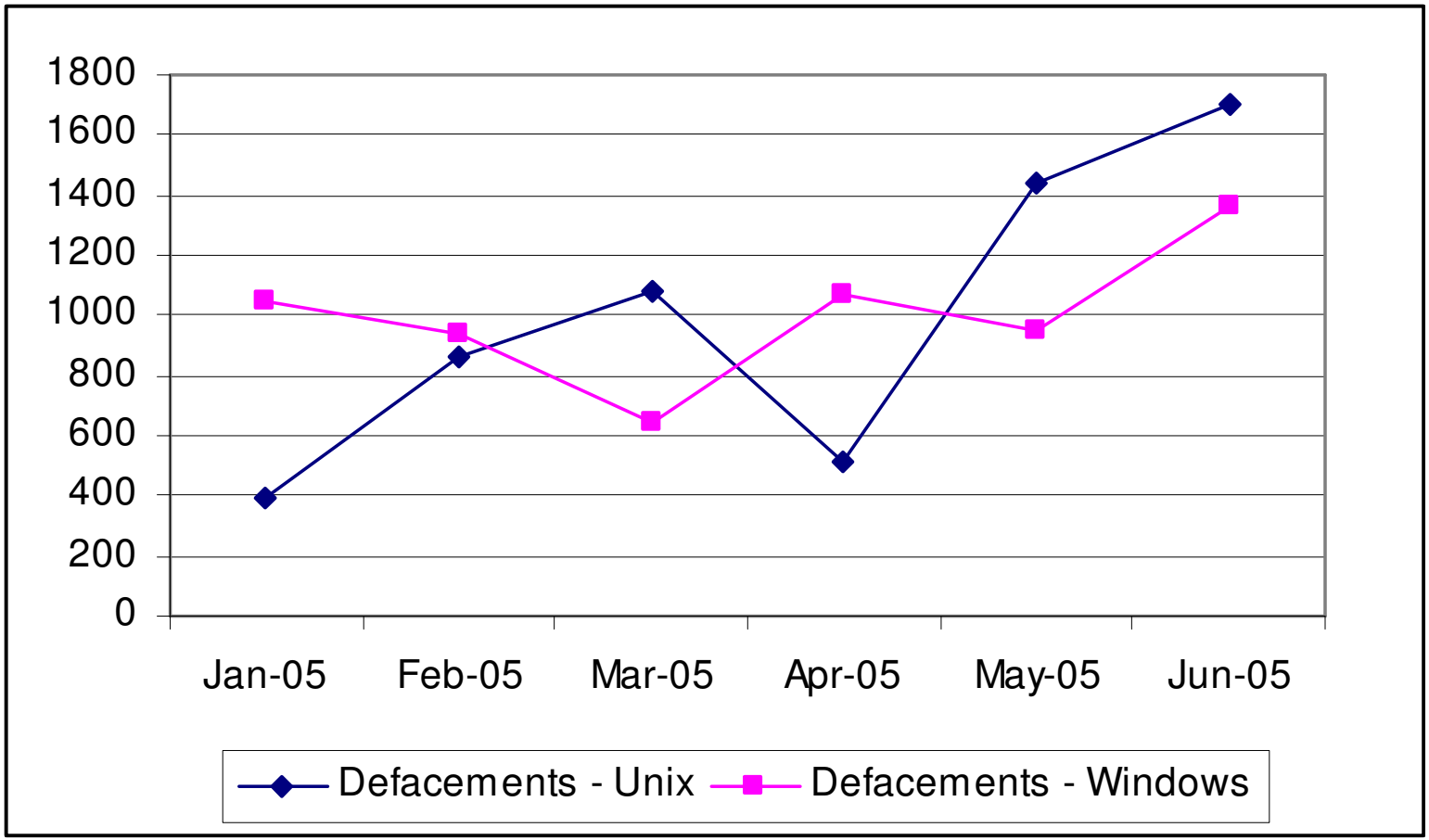
Threat Data
New Exploit Code Published & Shared



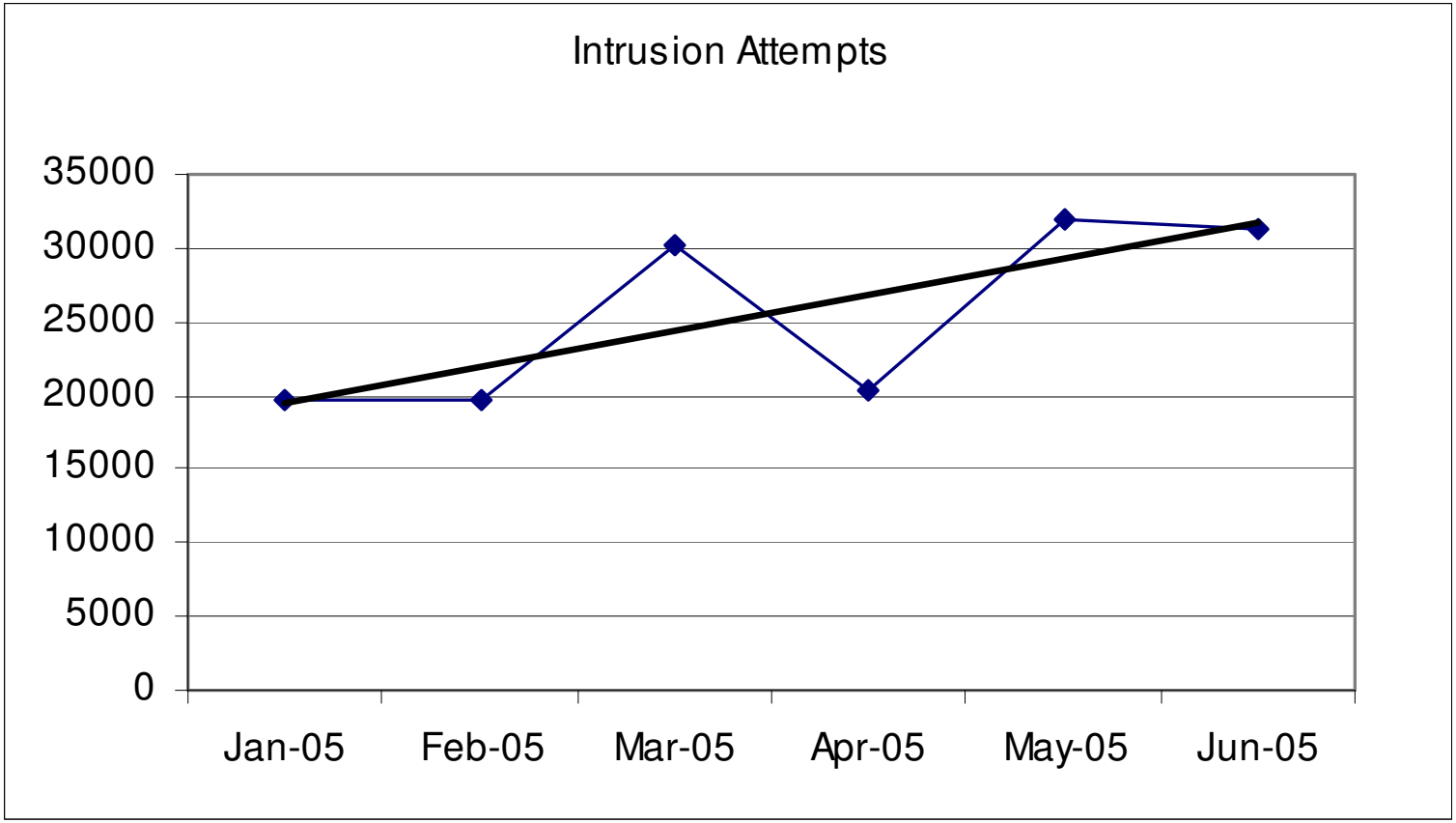
Threat Data
Unique Phishing Email Scams



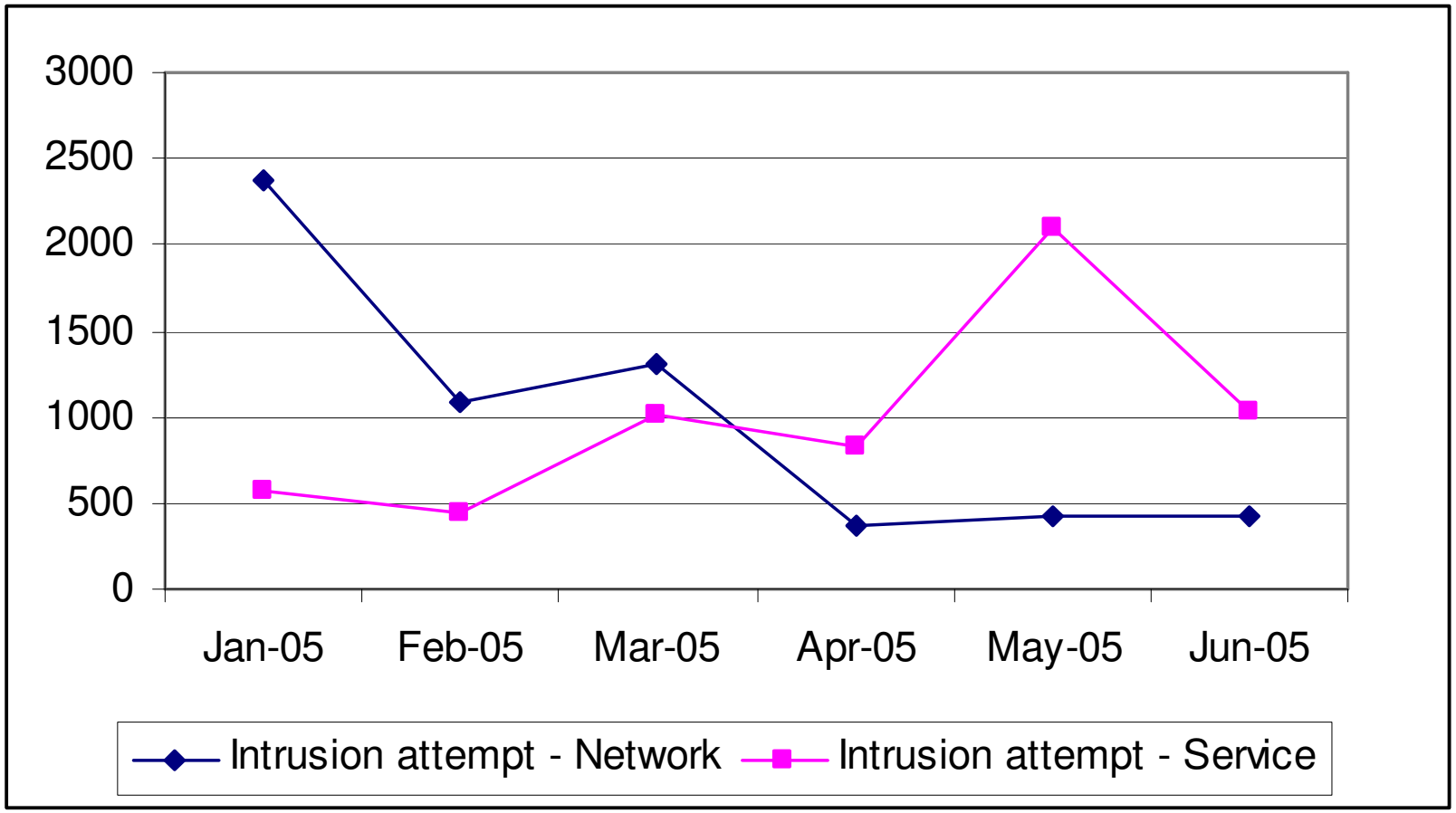
Threat Data
Successful Web Site Attacks Daily



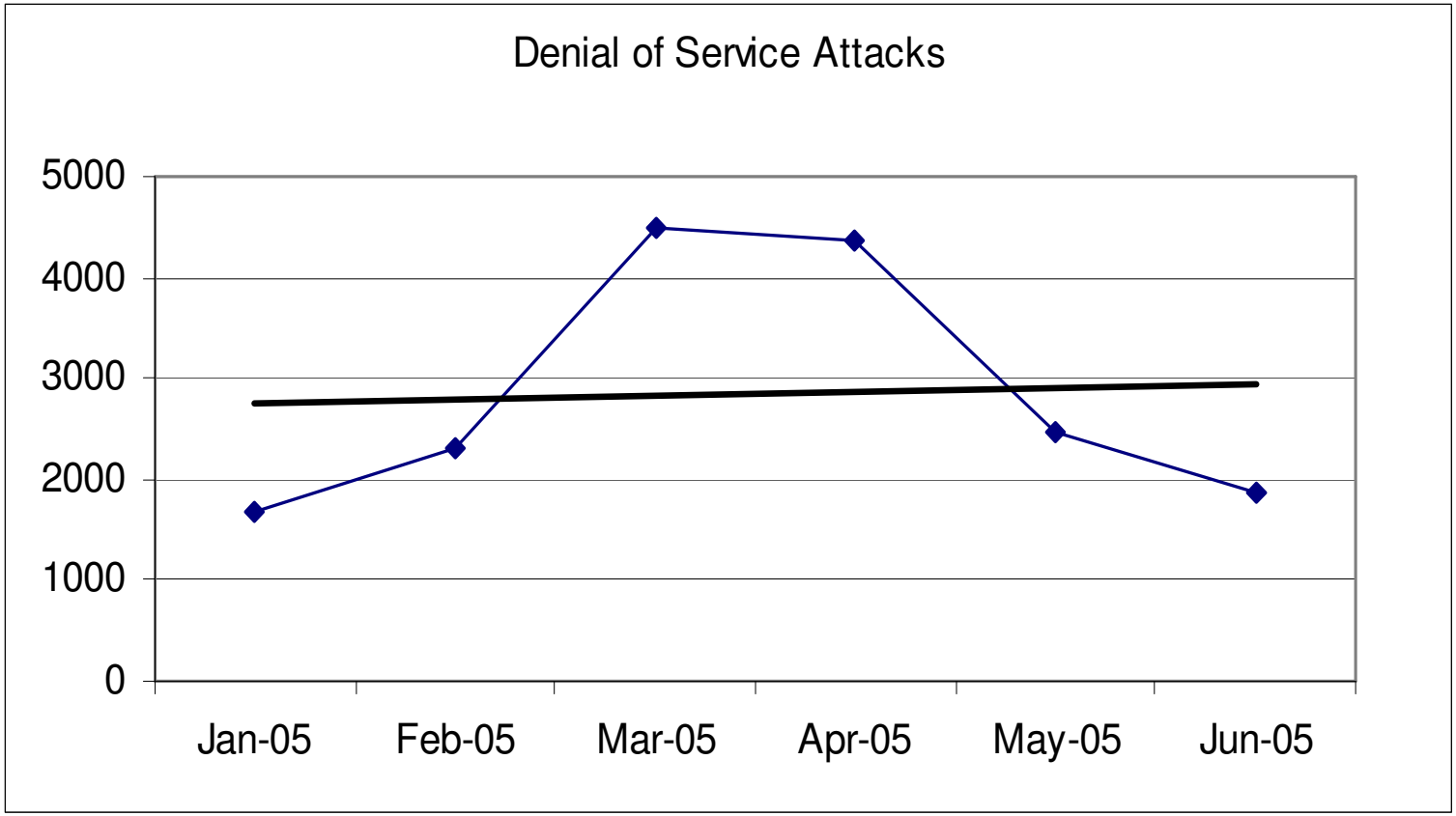
Threat Data
Intrusion Attempts



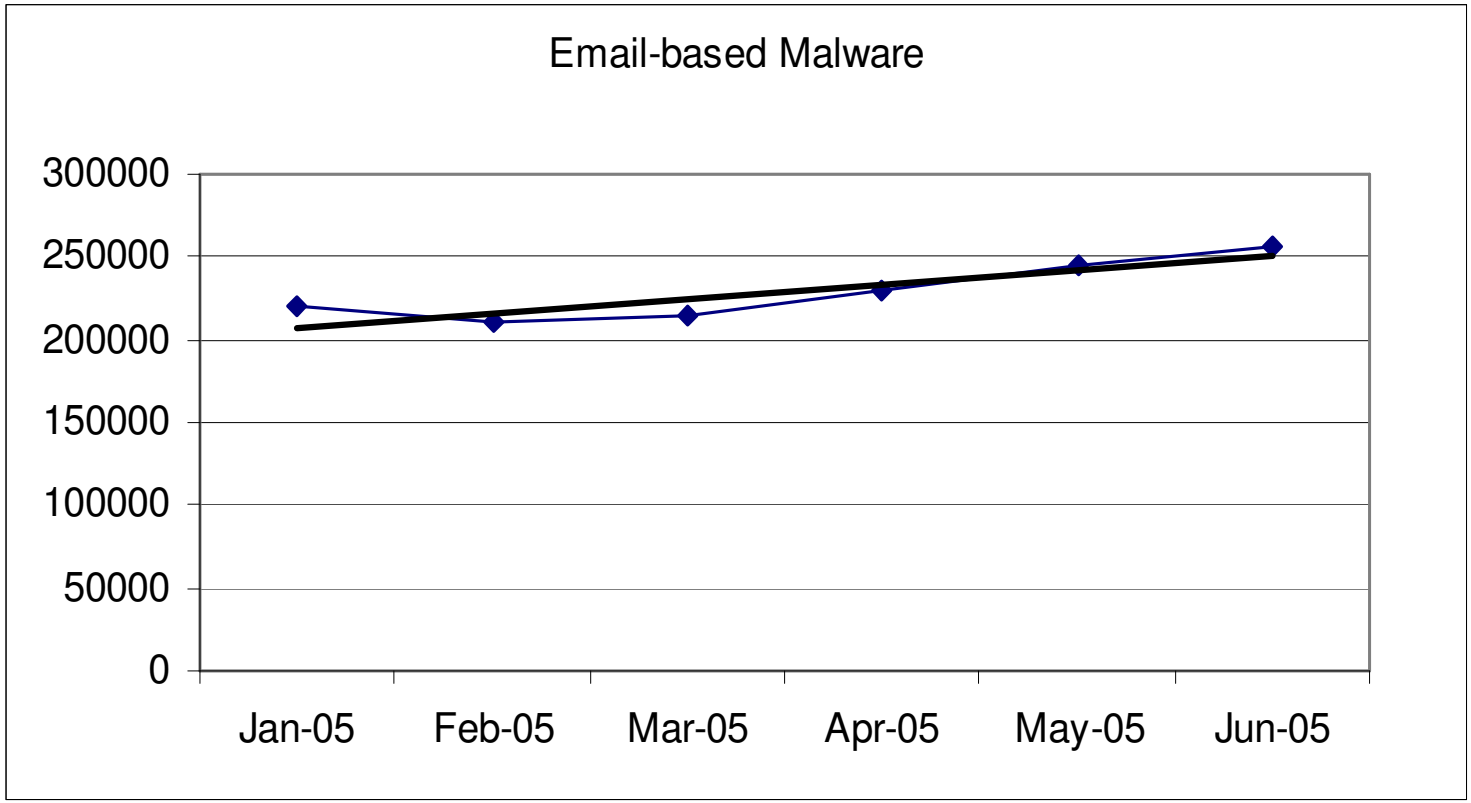
Threat Data
Intrusion Attempts Network vs. Application



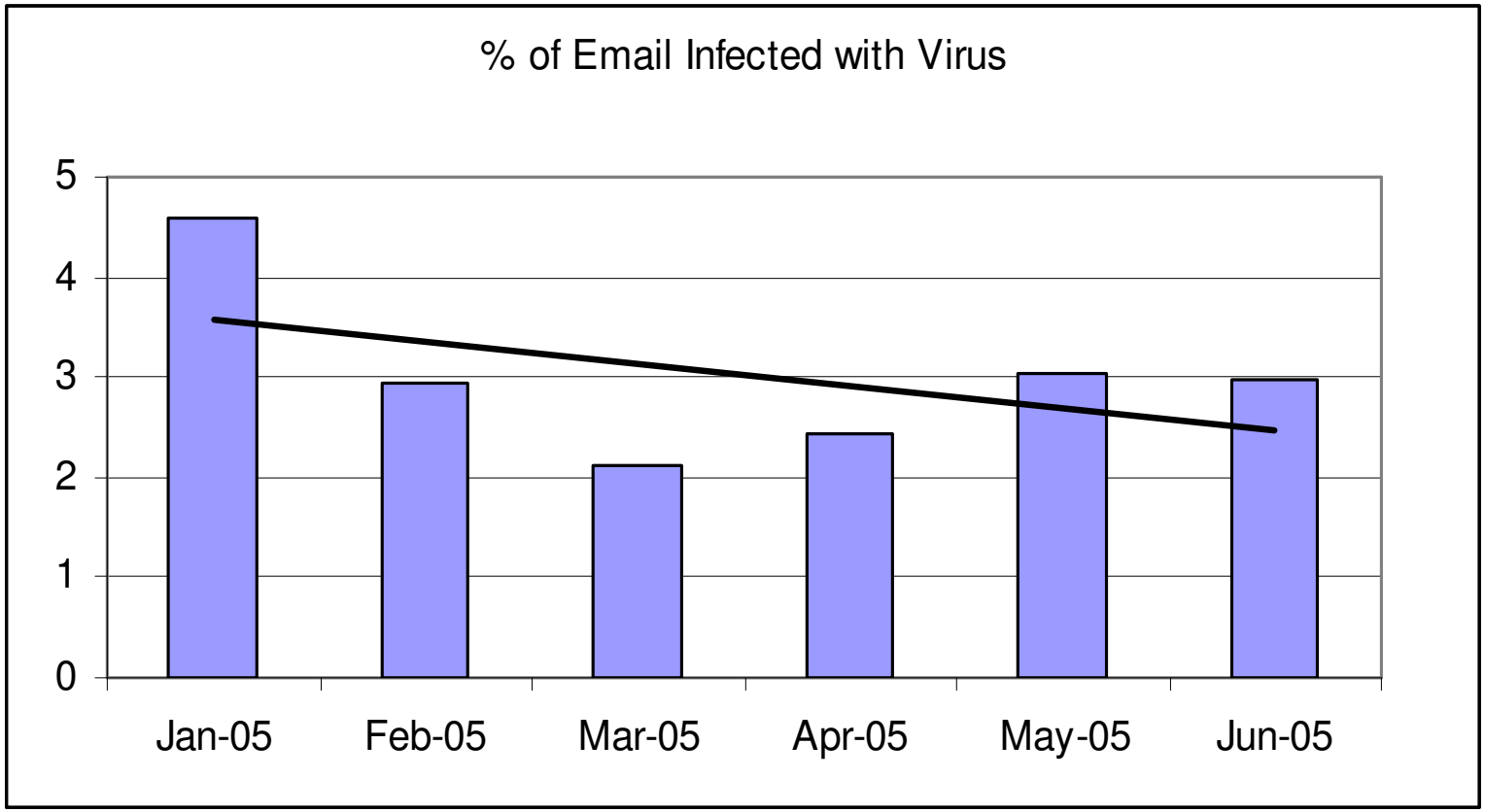
Threat Data
Denial of Service Attacks (Index)



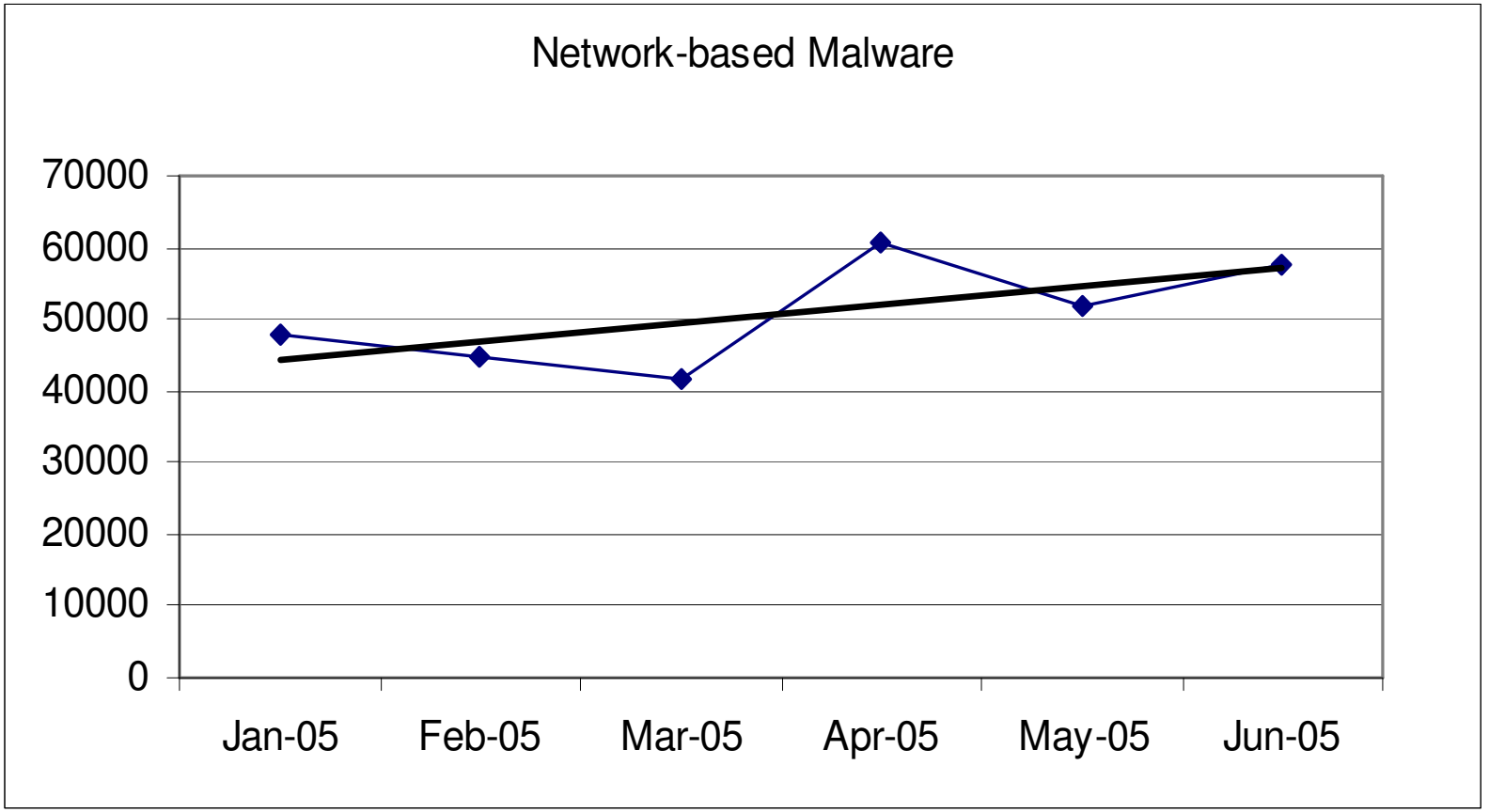
Threat Data
Email Based Malicious Code (Index)



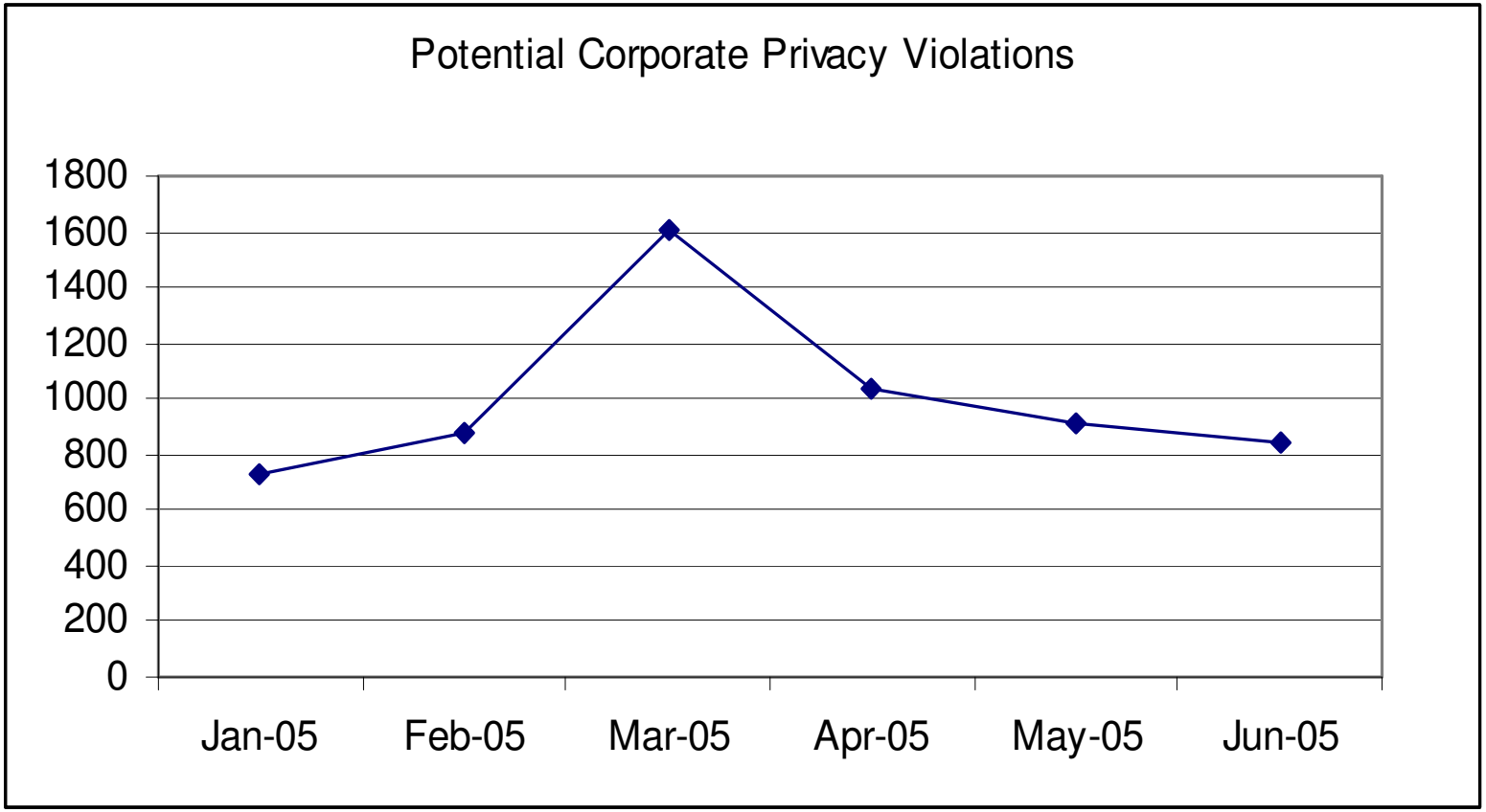
Threat Data
Email Based Malicious Code (Mail Metrics)



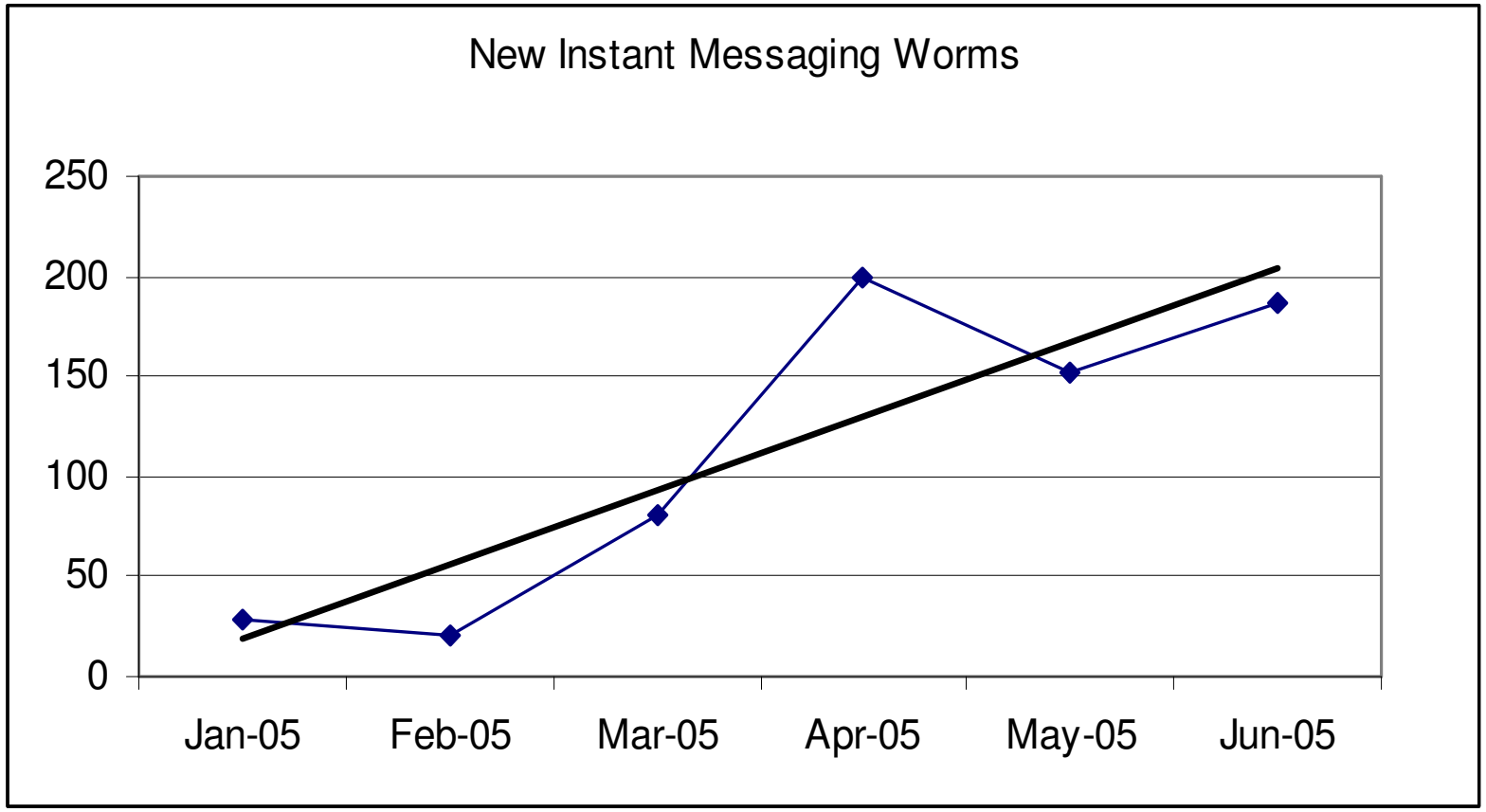
Threat Data
Network-type Malicious Code (Index)



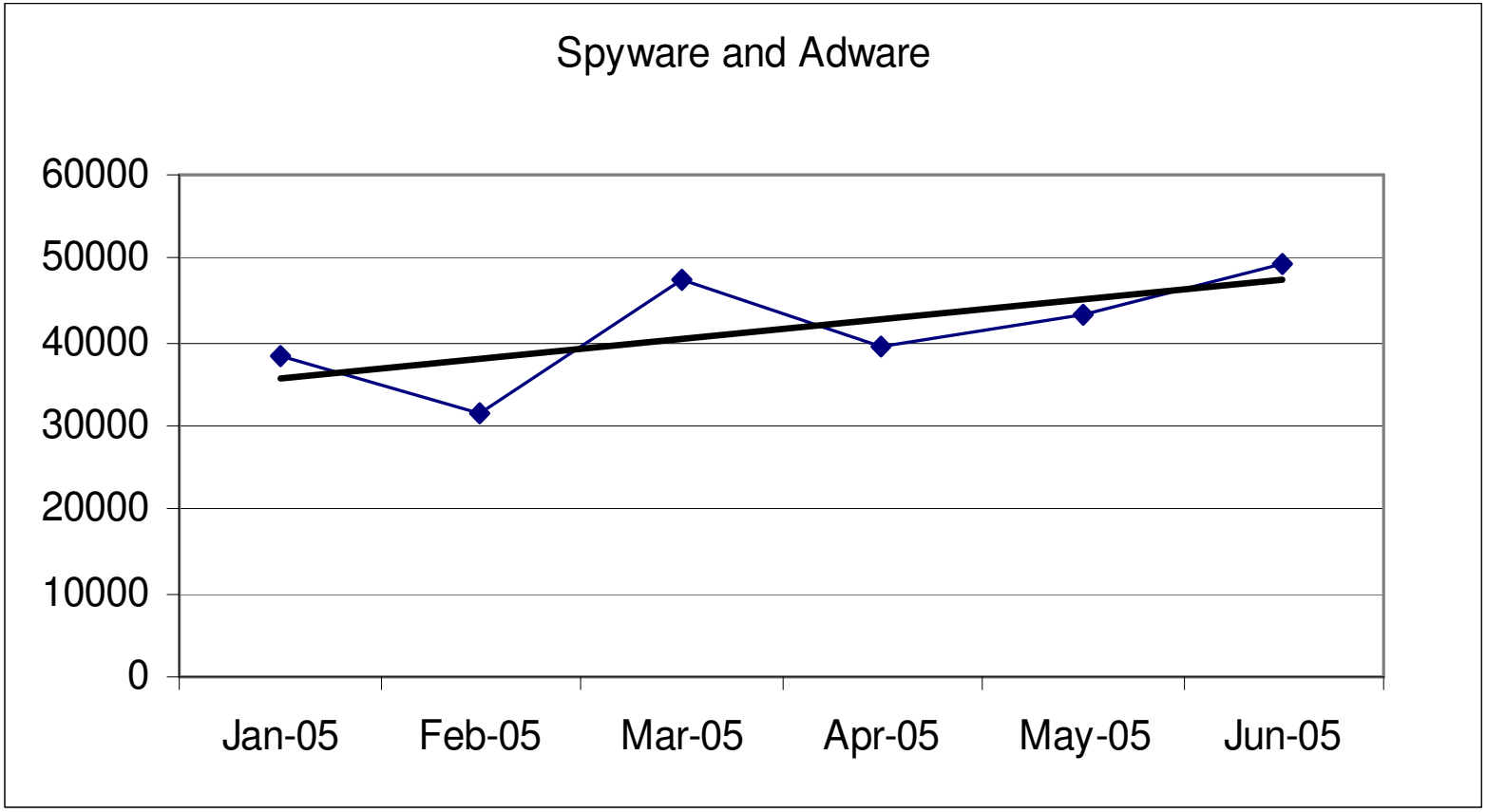
Compliance Data
Corporate Policy Violations



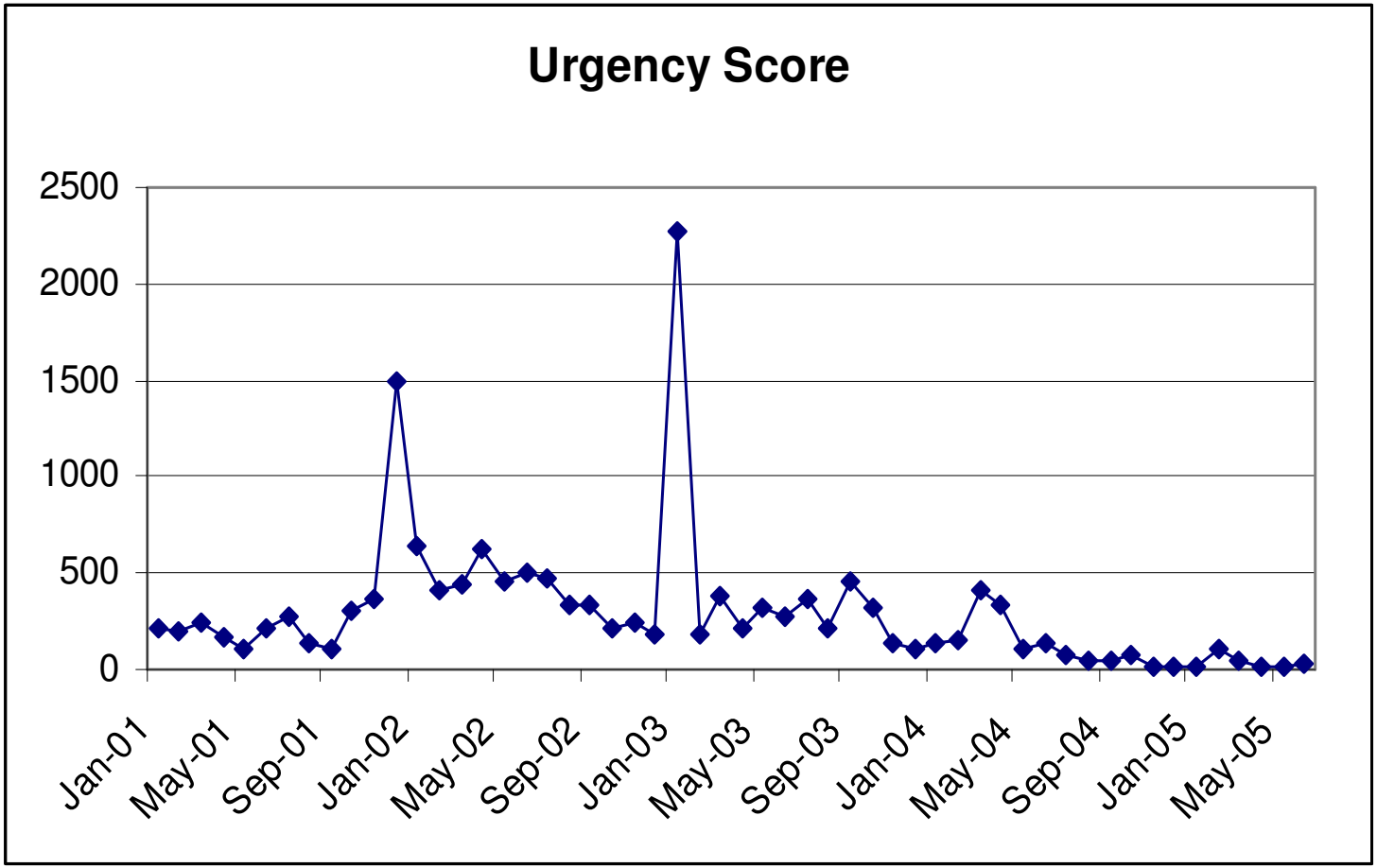
Threat Data
IM Malicious Code - New Worm Code Month



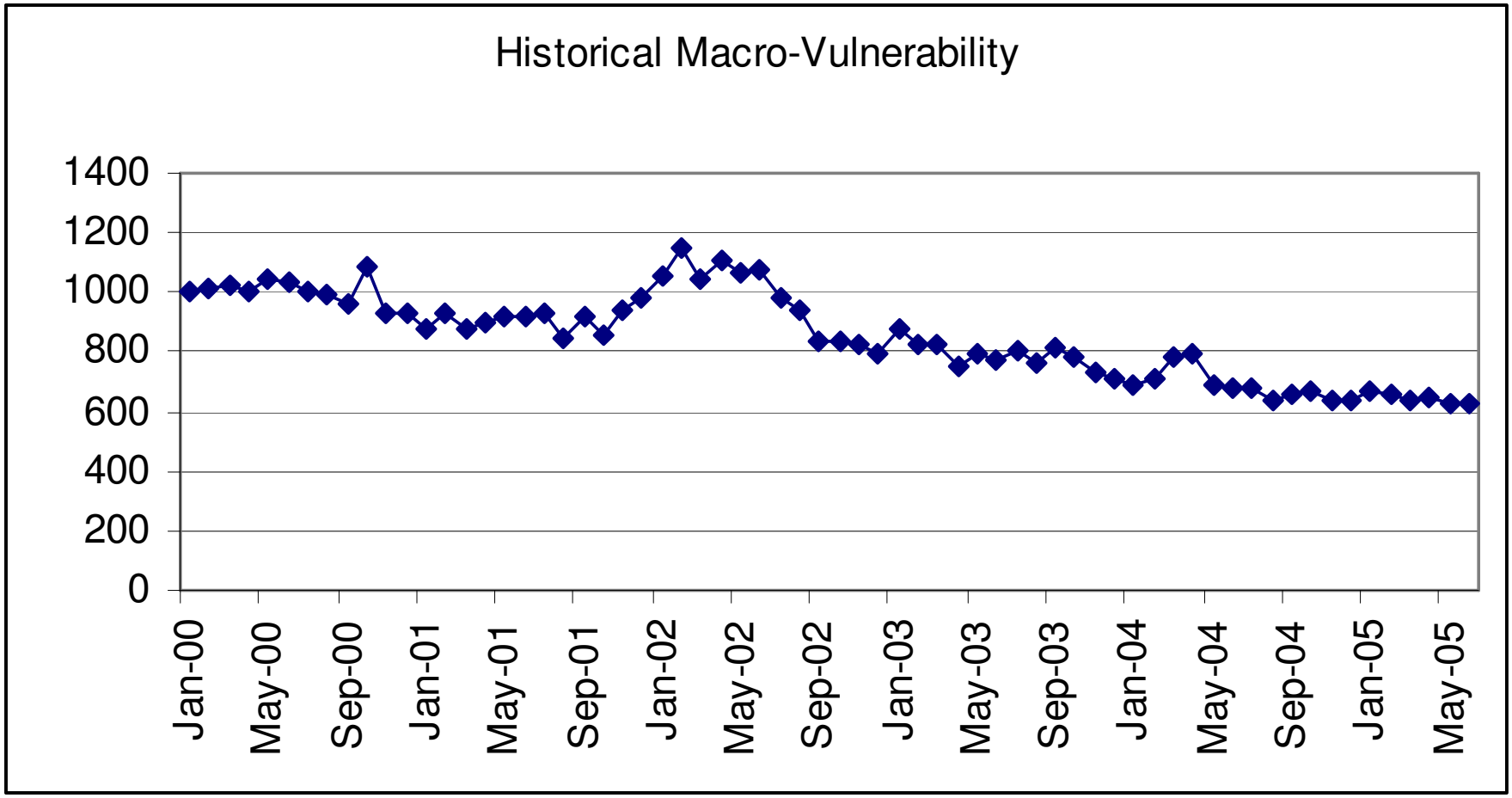
Threat Data
Malicious Code (Spyware Index)



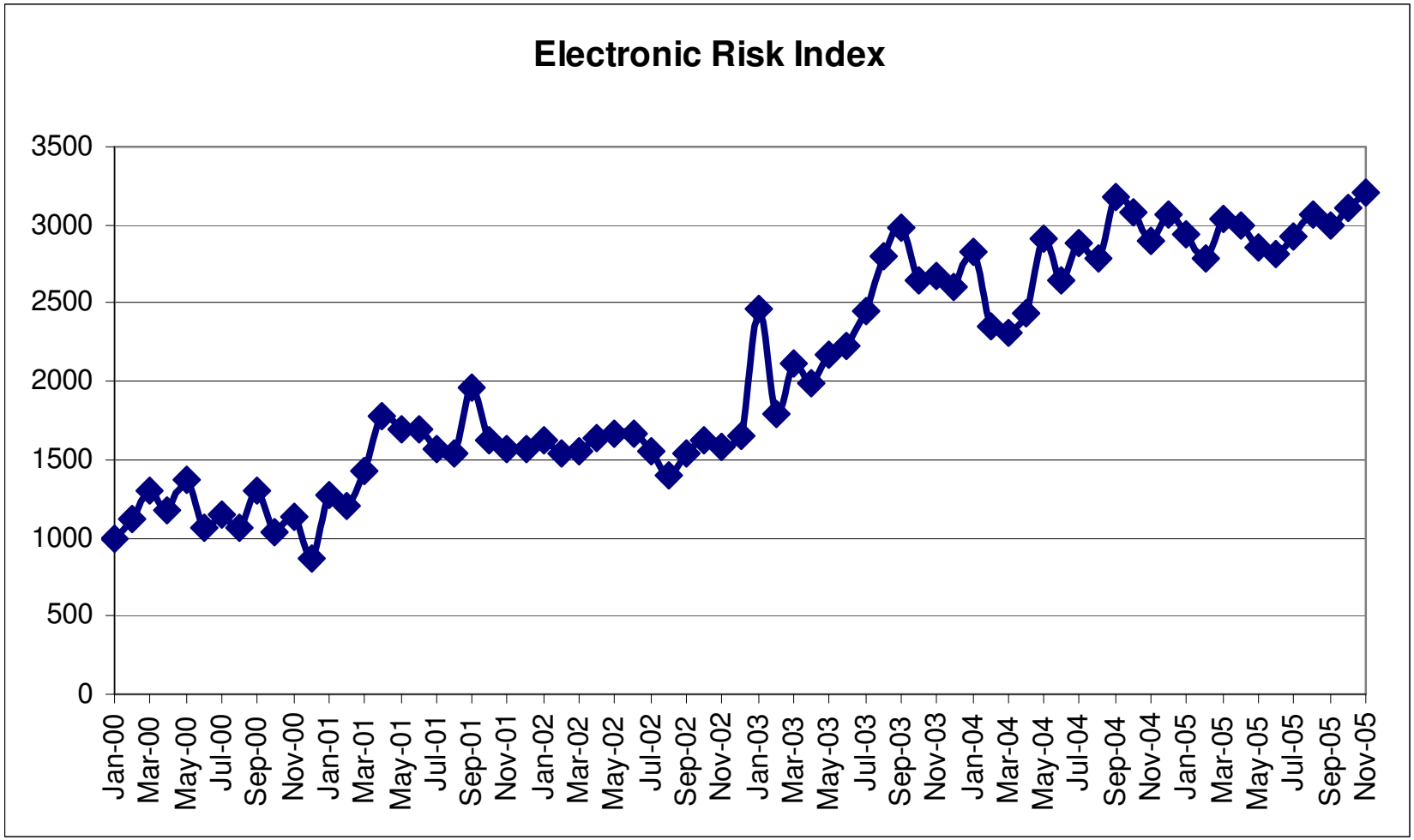
Risk Indicator Modifiers
Urgency in Corporate IT departments



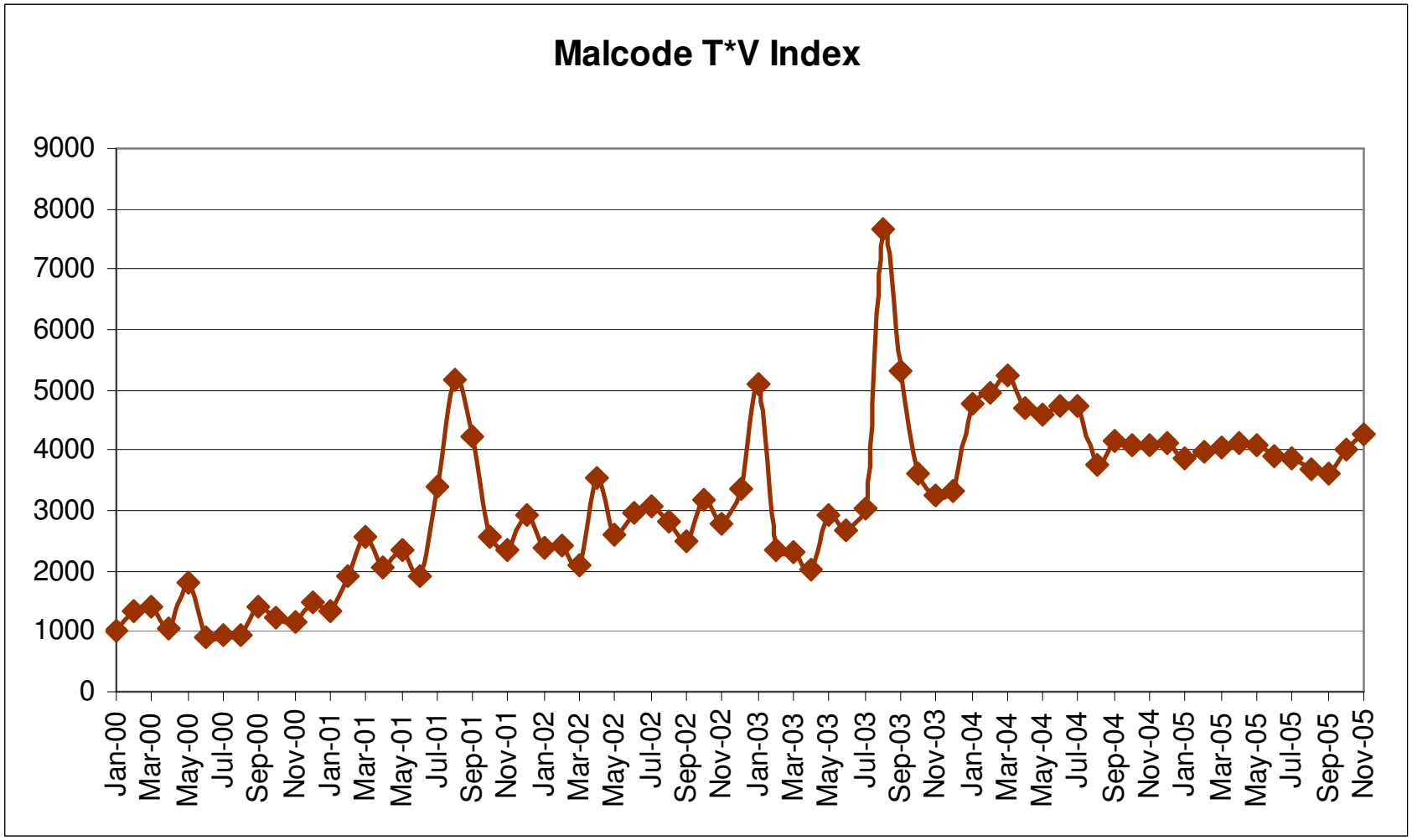
Vulnerability Data
Macro Vulnerabilities



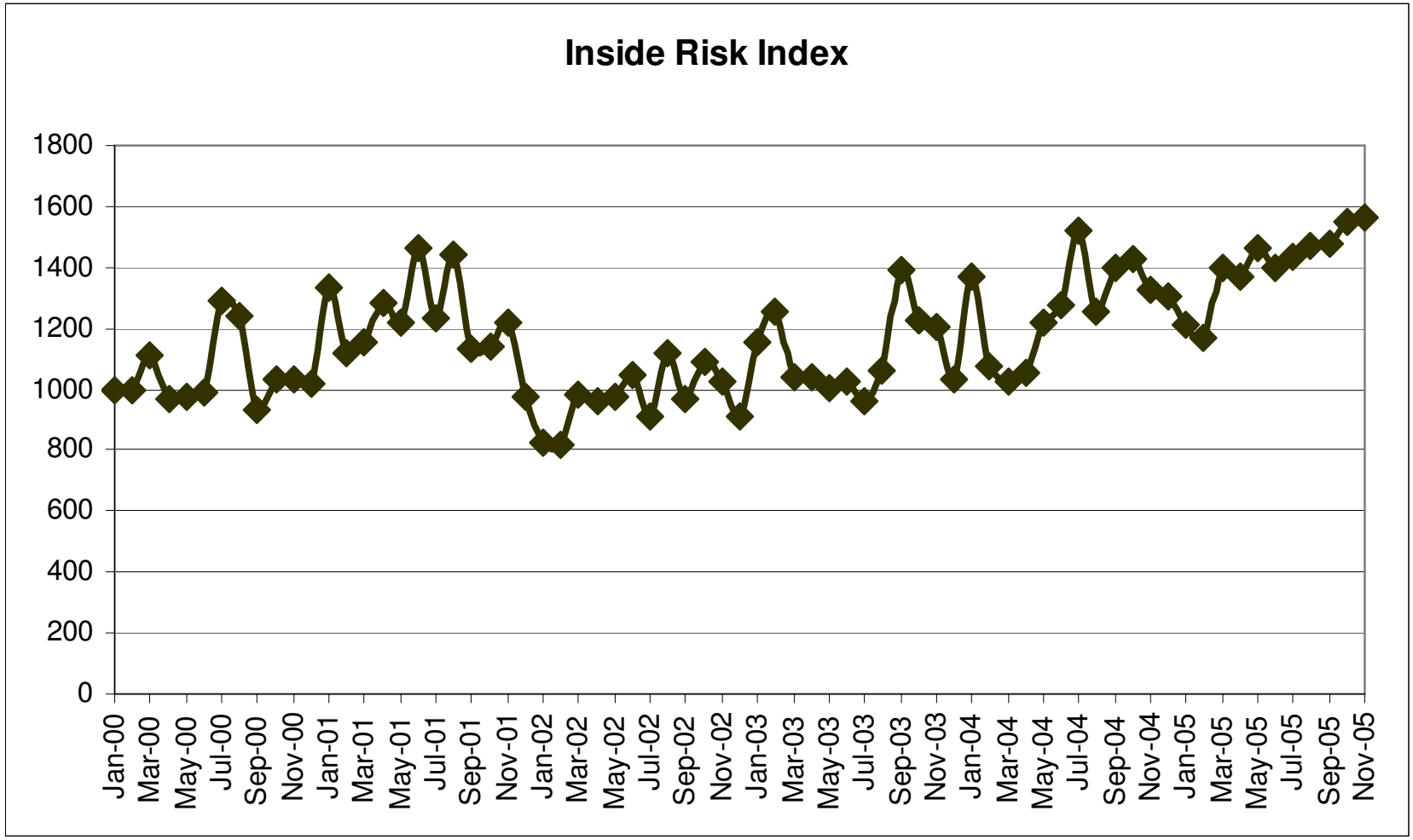
Growth in “Hacking” Risk to Enterprises Since 2000



Growth in Malicious Code Risk to Enterprises Since 2000



Growth in Insider Risk to Enterprises Since 2000



What is Wrong with our Security Thinking?

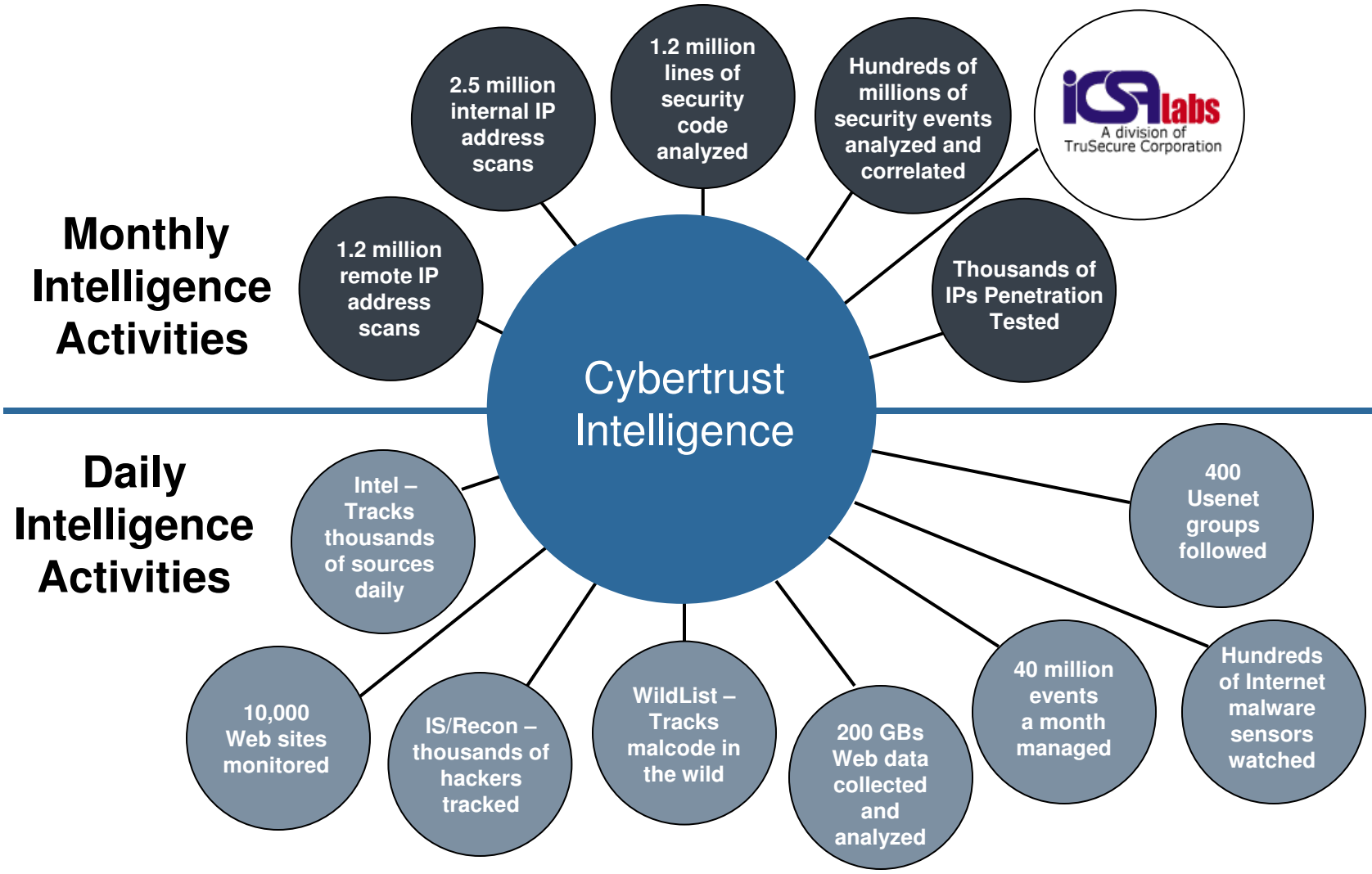
World is Flat	**World is Round**
Vulnerability	Risk
Single Computer	Community of Computers
Binary	Analog, Synergistic
Best Practices	Essential Practices

Sample Fallacies:

- ★ SLL (Internet encryption) fallacy
- ★ Longer passwords are stronger fallacy
- ★ Encrypting databases / disk drives reduces hacking risk fallacy
- Patching significantly reduces worm & mass attack risk fallacy
- Rapid anti-virus updates reduce risk fallacy
- Wireless at home increases risk for corporation fallacy
- Vulnerability Scanning & Patching of "Inside Computers" is among top 10 best countermeasures fallacy
- Policies like "don't double click" are worthless fallacies
- There is no Security in Obscurity fallacy

★ *Article or white paper available*

Applied Intelligence



Define Risk in a Measurable Way

The Cybertrust RISK EQUATION:

RISK = Threat * Vulnerability * Impact

(rate) (organizational) (event cost)

Risk (capital R) == ALE

- annualized loss expectancy

Risk = Threat * Vulnerability *Event Cost

Threat: (AKA Attack Rate)

- The ***Rate*** of potential *Security Events* (number of attempts per year, month, hour etc.)
- The ***Frequency*** that potential security events happen in a given time span
- Composed of world-wide rate modified by local Target Index, & other factors.
- *Cybertrust: Ballistic Threat Model, Threat Prediction*

Risk = Threat * Vulnerability * Event Cost

Vulnerability:

- The ***likelihood*** of success of a threat versus an **organization**.
  - A given computer is either vulnerable or not to a particular well defined threat (Vulnerability = 0 or 1).
- A given **organization** is composed of numerous targets (computers,people, rooms, paper) which, as a group, are variably vulnerable to a given threat category.
- Vulnerability is neither 0 nor 1 but is somewhere between and dynamically changes … So $0 < V < 1$
- *Cybertrust: Vulnerability Prevalence*
- *Threat Scenarios, Attack pathways, Vectors*

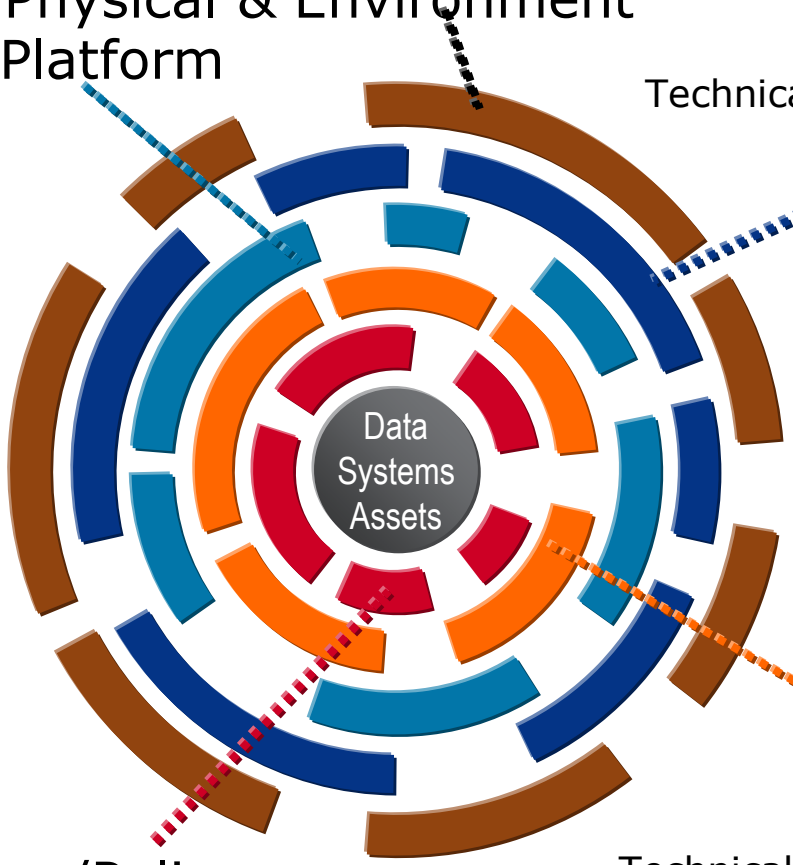
Risk = Threat * Vulnerability * Event Cost

Impact: (AKA Event Cost)

- Security Events result from a threat successfully exercised against a vulnerable organization.
- The total costs of all of the ramifications of a security event include both hard and soft costs.
- Total sum of all ramifications of a security event called Event Cost
- ***Impact = Total Dollars per Security Event***

Synergistic Controls

Effectiveness: $E_{total} = 1-((1-E_1)*(1-E_2)*(1-E_3)\ldots)$

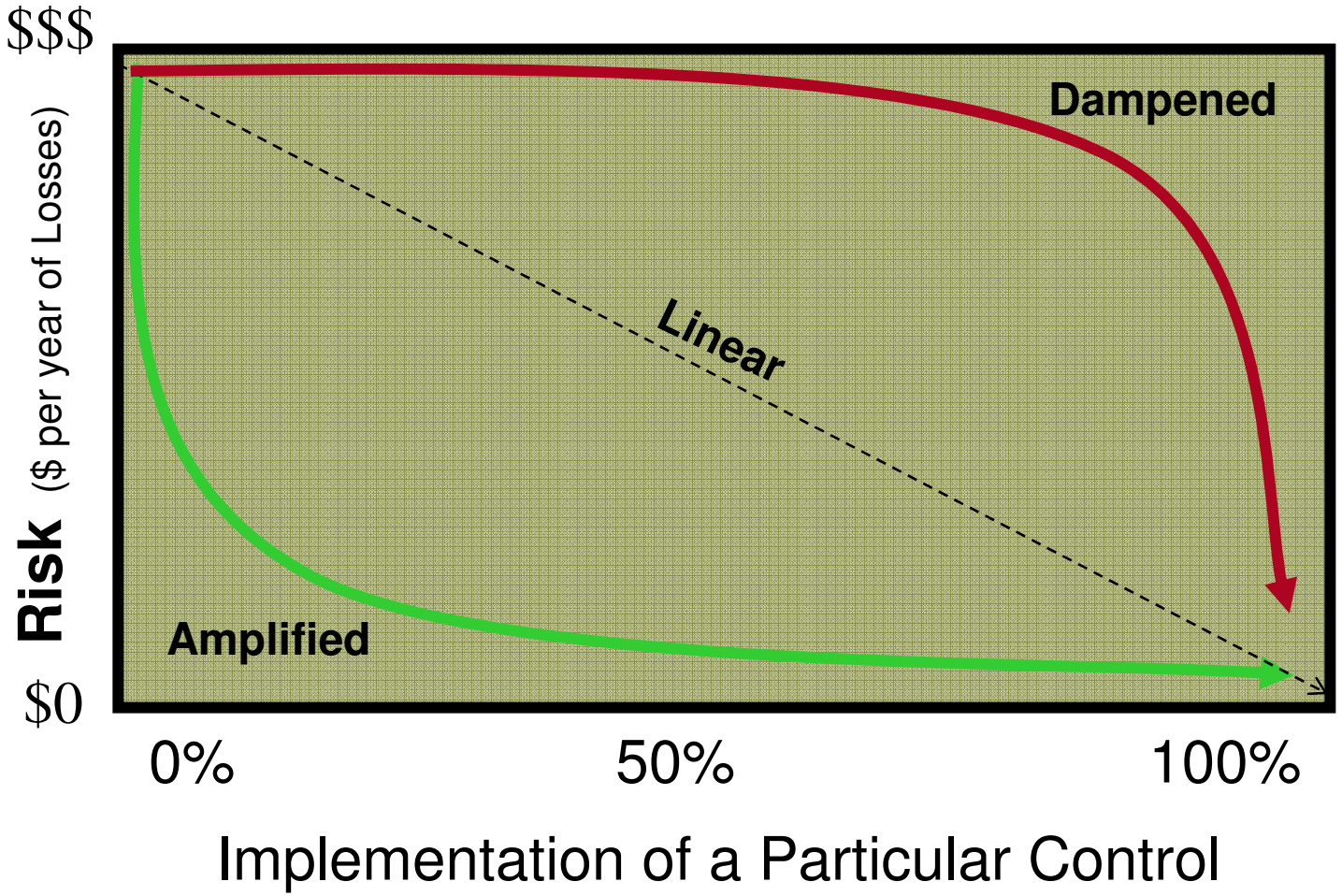


If Each control works at 80% effectiveness

Risk Reduction

99.97%

Risk vs. Extent of Control Implementation
In a community of assets



Control Risk with Countermeasures

Five Possible Types of Countermeasures

Deter	Reduces Threat Rate
Protect	Reduces Vulnerability
Detect	Reduces Cost
Recover	Reduces Cost
Transfer	Insurance (Reduces Net Cost)

We track and score effectiveness of first four in our Local Risk models

Cybertrust Seven Categories of Risk

45 Sub-Categories "threat scenarios" in current form

Electronic (External / Internal) Hacking, Sniffing, Spoofing….

MalCode - Viruses, Worms, Trojans, Spyware….

Privacy – corporate, employee, customer data

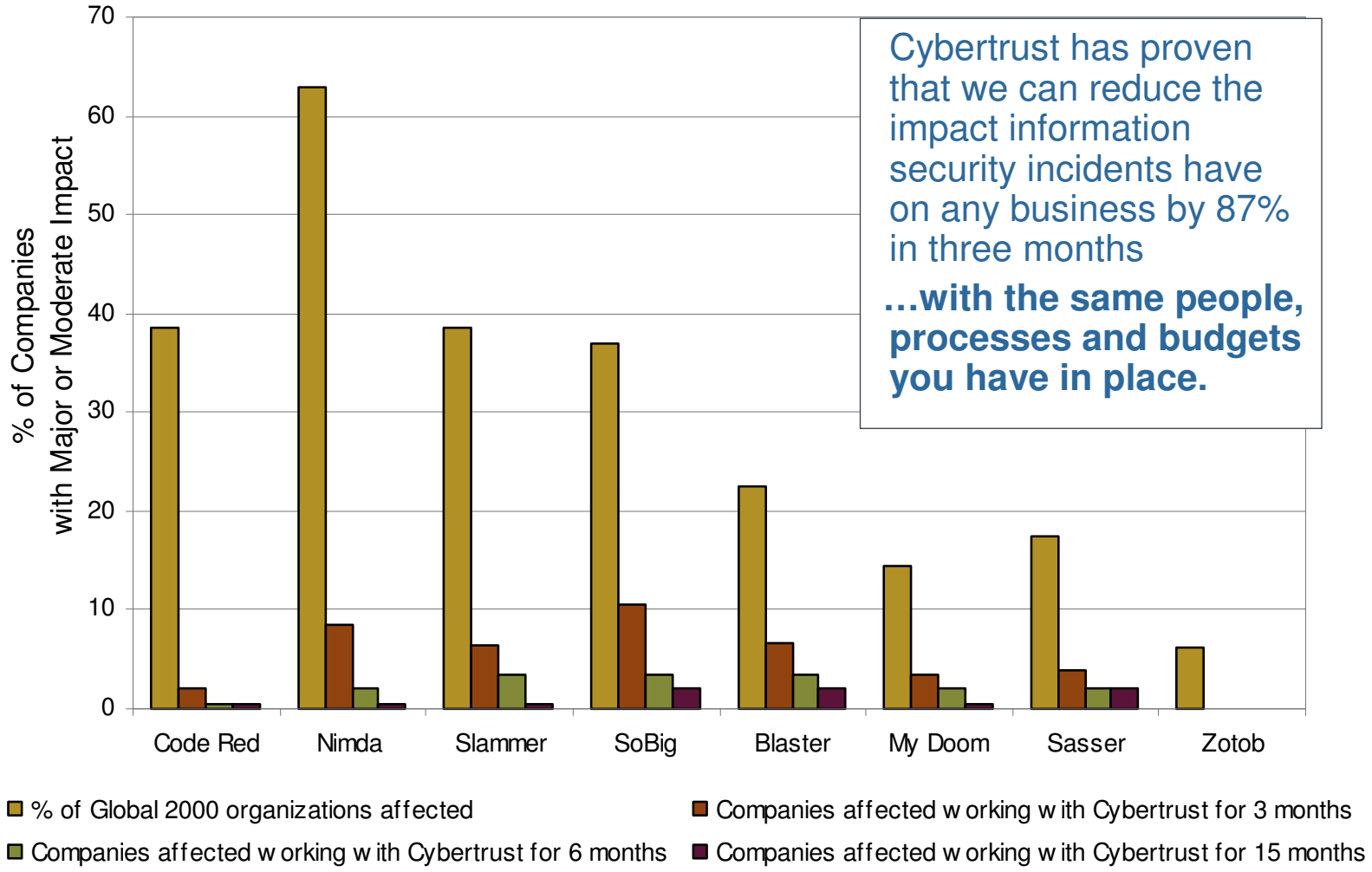
DownTime - DOS, Bugs, Power, Civil Unrest, Natural Disasters...

Physical - Theft, Terminal hijack…

Human - Social Engineering, Sticky-note, ….

Governance – Laws, Standards, Culture…

What Does That Mean to You?



Cybertrust has proven that we can reduce the impact information security incidents have on any business by 87% in three months

…with the same people, processes and budgets you have in place.