



IBM Global Services

The Evolving Threat

**Everything You Want to Know
but Were Afraid to Ask**

Sean Brantley

Security Sales Specialist Florida

(386) 562-2740

sbrantle@us.ibm.com



IBM Internet Security Systems®
Ahead of the threat.™



IBM Global Services

WARNING...

The content of this presentation is intended for mature audiences and may not be suitable for those security customers that “don’t want to know”!



IBM Internet Security Systems®
Ahead of the threat.™



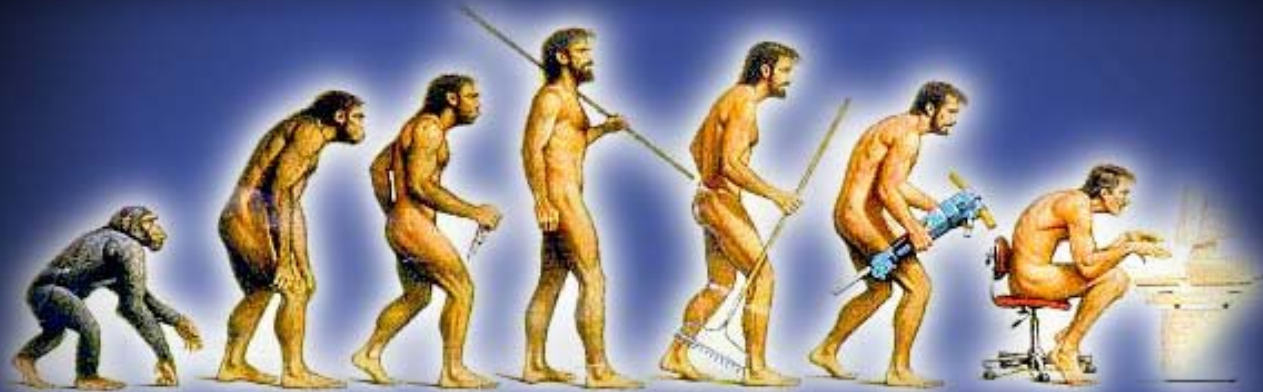
IBM Global Services

1. Change Happens...
2. The Threat has outgrown Legacy Defenses
3. We Must Adapt or _____

IBM Internet Security Systems®
Ahead of the threat.™

Change Happens...

- **Changes in the Impact of Data Loss**
- **Change within the Threat Landscape...**
- **Change within the Industry...**



What is the Financial Impacts for Data Loss?

- **The estimated cost is \$100 in per customer record!**
 - 1,000 customer records = \$100,000
 - 10,000 customer records = \$1,000,000
 - 50,000 customer records = \$5,000,000
 - 100,000 customer records = \$10,000,000

Note: This cost doesn't include law suits and or lose of customer!

What is the Leading Causes of Data Loss?

- The leading causes of sensitive data loss are due to three primary problems that include:
 - User errors
 - Violations of policy
 - Internet threats, attacks and hacks.

Florida Security Breach Notification Law

- Florida H.B. 481 (signed into law June 14, 2005) FLA. STAT.ch. 817.5681 Effective July 1, 2005
- (1)(a) Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph (10)(a), or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section. (b) Any person required to make notification under paragraph (a) who fails to do so within 45 days following the determination of a breach or receipt of notice from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed \$500,000, as follows:
 - 1. In the amount of \$1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days.
 - 2. If notification is not made within 180 days, any person required to make notification under paragraph (a) who fails to do so is subject to an administrative fine of up to \$500,000.

California Business Identity Theft Law

- Theft of Business Identity Is Felony Under Bill Signed By Schwarzenegger
- SACRAMENTO, Calif.--Gov. Arnold Schwarzenegger (R) signed a bill Feb. 25 that makes it a felony to steal the identity of a business entity--adding businesses to the definition of "person" in the state's identity theft provisions of the Penal Code.
- A.B. 424, by Assemblyman Ronald S. Calderon (D), takes effect immediately. It expands the definition of a person to include a firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity. Those convicted of identity theft face up to three years in prison and fines up to \$10,000.
- The measure was sponsored by Attorney General Bill Lockyer (D). According to Lockyer, the measure addresses a growing trend in identity theft: taking over the identity of a business. Because businesses make larger purchases and often have more available credit than individuals, thieves that take over a business identity can steal more merchandise or cash without raising suspicions.

Recent Data Breaches

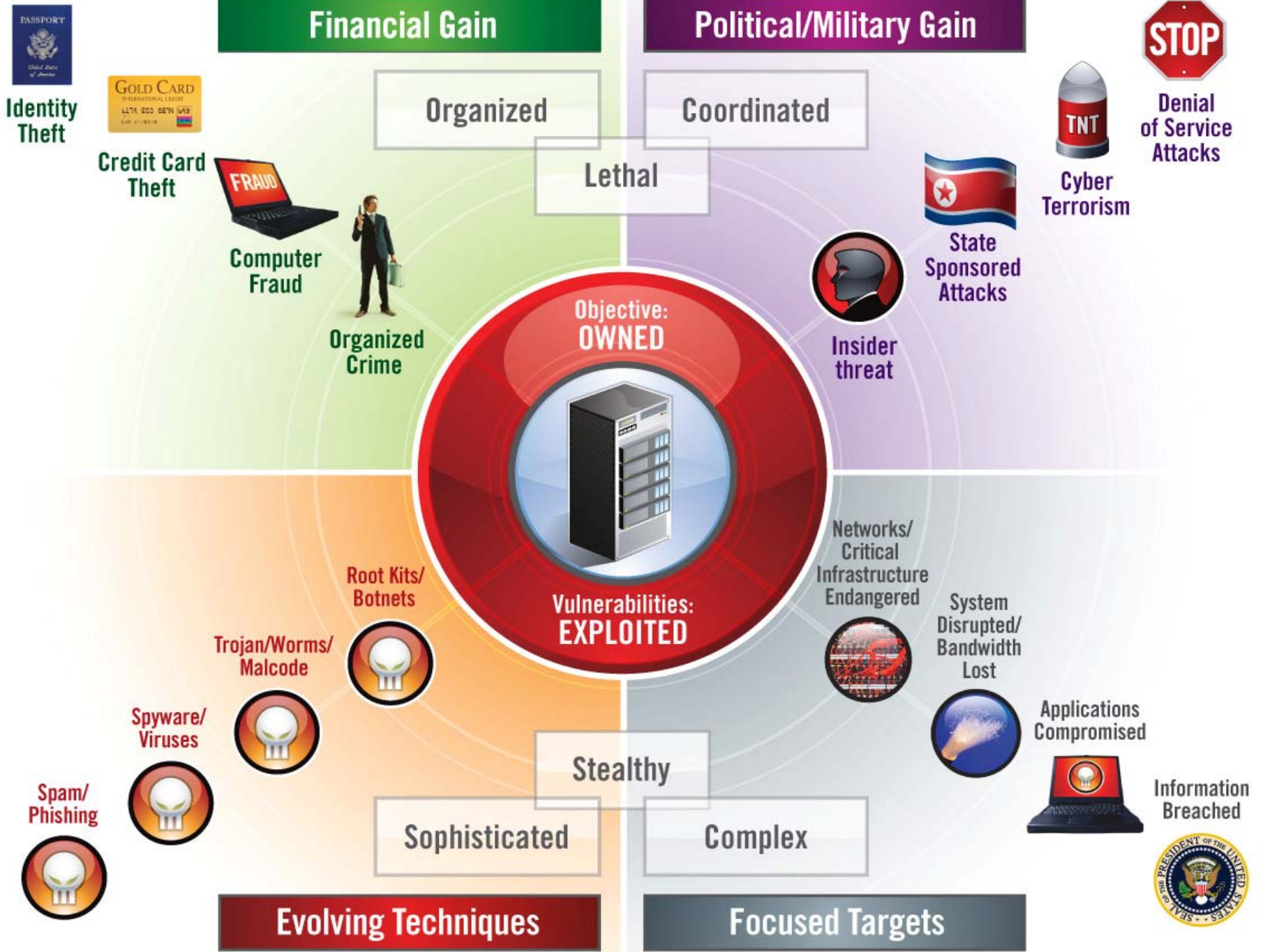
- Jan. 12, 2007 MoneyGram International (Minneapolis, MN)
MoneyGram, a payment service provider, reported that a company server was unlawfully accessed over the Internet last month. It contained information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.
- Sept. 9, 2006 Cleveland Clinic (Naples, FL)
A clinic employee stole the personal information of 1,100 patients from electronic files and sold it to her cousin, owner of Advanced Medical Claims, who used it to file fraudulent Medicare claims totaling more than \$2.8 million. Information included names, SSNs, birthdates, addresses and other details. Both individuals were indicted.
- Mar. 3, 2007 Johnny's Selected Seeds (Winslow, ME) Hacker accessed credit card account information of 11,500 online customers. About 20 credit cards have been used fraudulently.

Recent Data Breaches

- Oct. 26, 2006 Akron Children's Hospital (Akron, OH) Overseas hackers broke into two computers at Children's Hospital. One contained private patient data (including Social Security numbers) and the other held billing and banking information. Total lost was 235,903 records.
- Jan. 12, 2007 MoneyGram International (Minneapolis, MN) MoneyGram, a payment service provider, reported that a company server was unlawfully accessed over the Internet last month. It contained information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.
- Feb. 8, 2007 St. Mary's Hospital (Leonardtown, MD) A laptop was stolen in December that contained 130,000 names, SSNs, and birthdates for many of the Hospital's patients.

Standard Incident Response Methodology

- There are a number of different incident response methodologies that can be found on the Internet. Generally, these methodologies will consist of the following phases;
- Planning
- Identification
- Confirmation
- Containment
- Preservation
- Analysis
- Eradication
- Remediation
- Reporting
- The methodology chosen by an organization or vendor should conform to best practices such as ISO 17799 (27001).



What sparked all of this?

- Shift from “Glory-Motivated-Vandals” to “Financially-Politically-Motivated-Cyber-Crime”
- “Designer Worms” and “Designer Trojans”
- The Bot-Networks (Worms → Bots)
- Undermining Traditional AV, Firewall, IDS



The Old Enemy



Chen-Ing Hau
CIH Virus



Joseph McElroy
Hacked US Dept
of Energy



Jeffrey Lee Parson
Blaster-B copycat

The New Enemy



Jeremy Jaynes
\$24M SPAM KING



Jay Echouafni
Competitive DDoS



Andrew Schwarmkoff
Russian Mob Phisher

Quote from the Enemy



Kevin Mitnick

**Convicted in 1995 for
hacking into**

Motorola and Nokia

Source: CNN News Online October 13, 2005

CNN: Compared to the time you were an illegal hacker, and the contemporary landscape, how easy is it to hack a computer? Has security improved much? Would you still be able to do what you did years ago?

MITNICK: I get hired to hack into computers now and sometimes it's actually easier than it was years ago. It really depends on who the client is -- or if you're doing ethical hacking, who the target is. It could be a difficult target or an easy target. The security landscape, the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same. So, it depends how vigilant the owners and the operators of the computer systems and the network are, and it really doesn't go to the question of are we living in a more secure world? We are not living in a more secure world.



IBM Global Services

1. Change Happens...

**2. The Threat has Outgrown
Legacy Defenses**

3. Adapt or _____

IBM Internet Security Systems®
Ahead of the threat.™

Security Challenges...

Business Facts

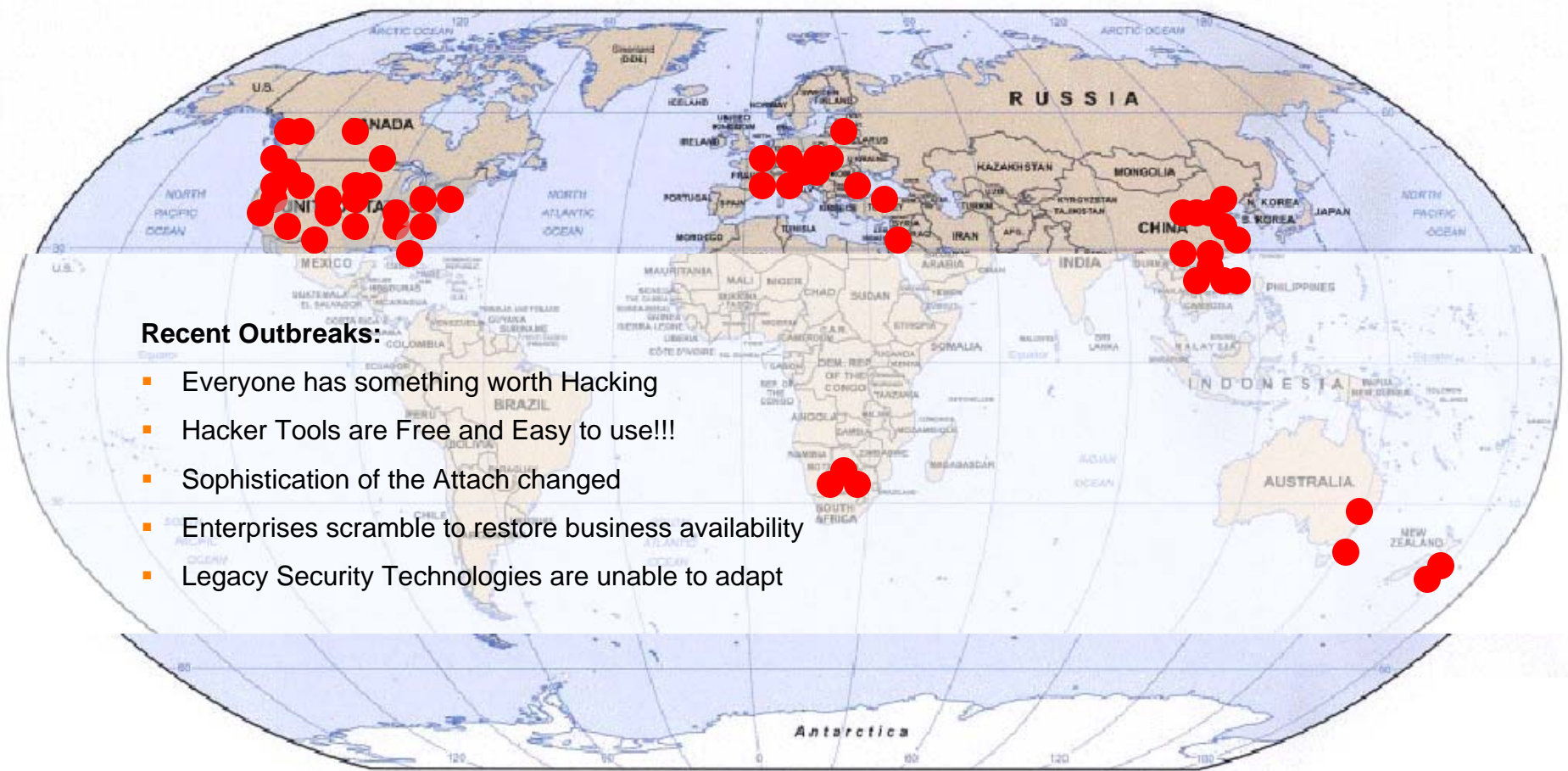
- Expanding Threat Landscape
- Limited Resources
- Increasingly Complex Networks
- Need for Total Risk Management
- Need to Report on Compliance
- Use of Technology for Automation



Impediments to Success

- Growing Vulnerabilities
- Mobile Assets
- Network Definition is Increasing
- Time Between Vulnerability and Exploit is decreasing
- Need to Report on Compliance

The Speed of Attacks Accelerates



Recent Outbreaks:

- Everyone has something worth Hacking
- Hacker Tools are Free and Easy to use!!!
- Sophistication of the Attack changed
- Enterprises scramble to restore business availability
- Legacy Security Technologies are unable to adapt

An explosion of innovation in Malicious Code...



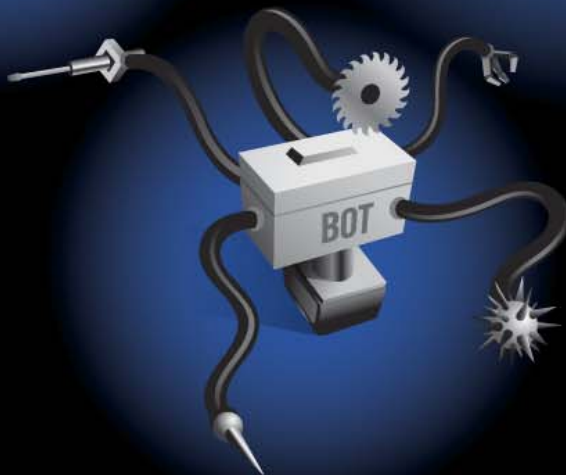
©IBM Internet Security Systems



©IBM Internet Security Systems



©IBM Internet Security Systems



©IBM Internet Security Systems



©IBM Internet Security Systems

MalCode does not NEED vulnerabilities

From SOPHOS: More MalCode – Mostly Trojans

The numbers of malware increased, and the growing emphasis on secrecy and stealth that we saw at the end of last year has continued to spiral upwards. Spyware and phishing remain two of the biggest threats that businesses now face, and malware attacks are almost universally targeted to the mass-mailing and drawing unneeded attention. The CIOs of 2006 by the Deloitte Touche Tohmatsu (78%, up from 68% in 2005) security breaches identified

Trojans are now 75-80% of the new MalCode

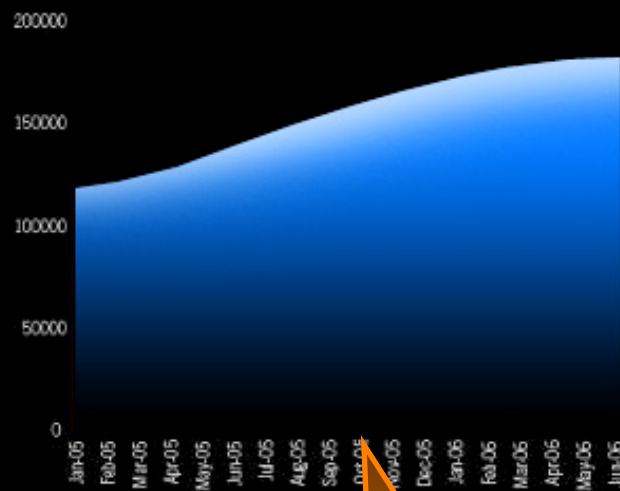


Figure 1: Growth of malware

Malware authors are increasingly moving away from email-aware worms to their search for victims to infect millions of computers, and increase their own protection. Similar to the volume of spam attacks under the radar of security software, the volume of malware is increasing. Sophos estimates that every 35 emails are viral for the same period in 2005 – further proof that email worm

They nearly DOUBLED the prior 21 years to >200,000

- 6 months at a glance
- Over 180,000 threats detected by Sophos
- Viral emails down to 1 in 91
- New Trojans outweigh viruses and worms 4:1**
- Ransomware demands money with menace

2007 Outlook – Malcode Trends

- **Continued shift towards profit**
 - PWS's, Keyloggers, Ransomware
- **Continued release of 0-Day exploits with Shellcode (MalCONTENT)**
- **Increased investment and innovation in MalCODE**
- **Increase in use of script based droppers**
 - Encrypted and polymorphic scripts
- **Increasing stealth techniques**
 - 3 RootKit POC's being examined by malcode underworld
 - VMWare Rootkit – SubVirt
 - BIOS Rootkit
 - Boot Sector Rootkit



IBM Global Services

1. Change Happens...
2. The Threat has outgrown Legacy Defenses
3. Adapt or _____

IBM Internet Security Systems®
Ahead of the threat.™

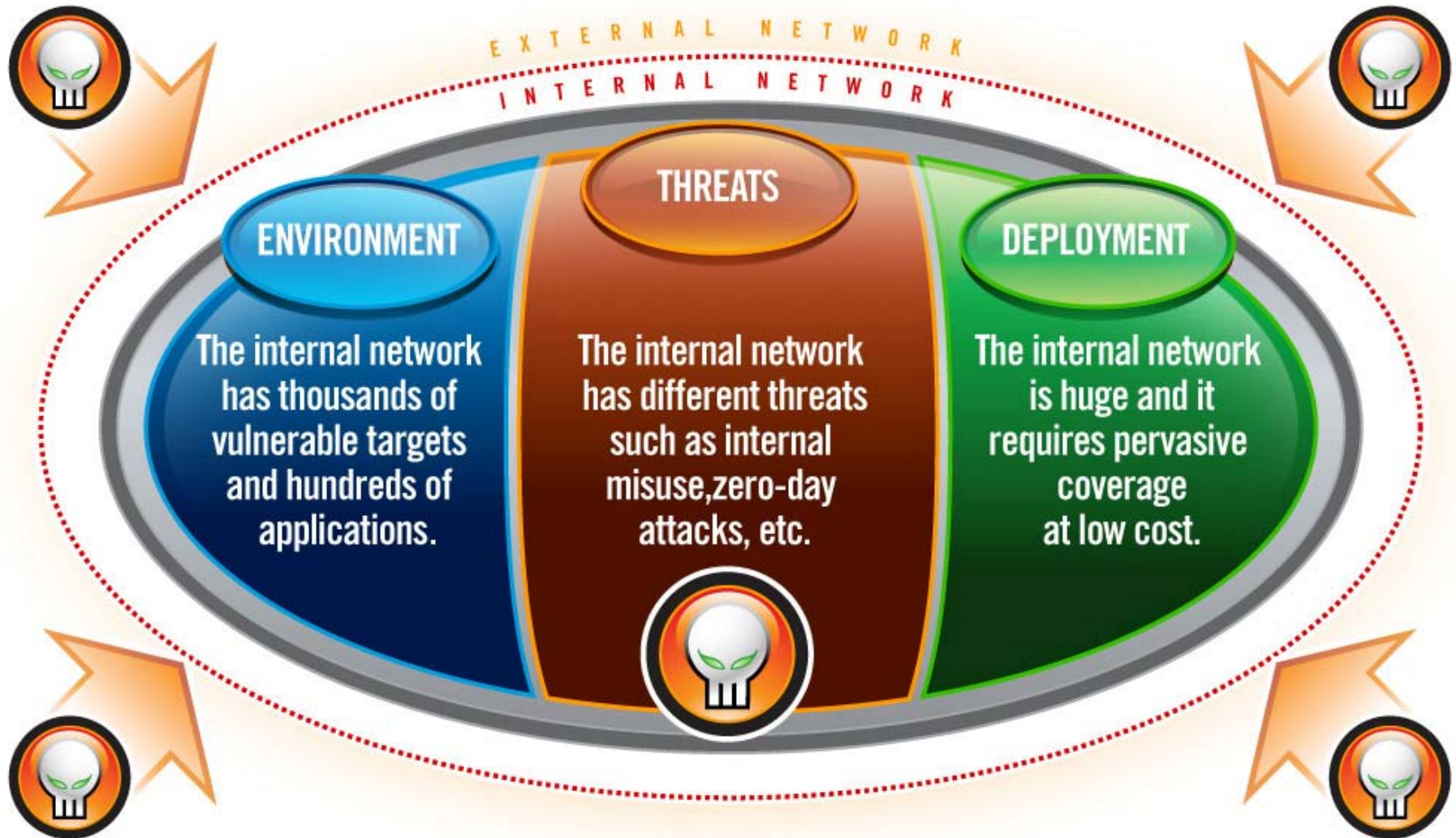
Has your Security Evolved?

- **The threats are rapidly evolving...has your protection?**
 - Re-evaluate antiquated security agent effectiveness against evolving threats
- **Many Threats CANNOT be detected with our Legacy Security Solutions**
- **Single technologies cannot adequately protect**
- **Need multi-layered approach**
- **Educate ourselves on new, more capable technologies**

Your Plan of Attack in 2007

- **Get an Independent Security Assessment Done Annually**
- **Create a Standard Incident Response Methodology**
 - Hire a third part consultant
 - Host quarterly incident response drills
- **Protect against the Insider Threat**
 - Implement Behavior/Anomaly detection technology to watch for the Insider threat
 - Invest in Internal Assessment tools
- **Create Internal Security Domains**
 - Protection from malicious activity with Network Based IPS
 - End Node Asset Protection with Host based IPS
- **Purchase Security Technologies with Consolidated Command and Control**
- **Control the Access and Identity of User in your Environment**
- **Get E-mal protection in place now!**
 - Outsourcing mail scanning the fastest and simplest way to fix this problem!
- **Reduce the Number of Security Vendors you Employee**
- **Should Consider Investing in a Security Manager Server Provider**
- **Web Proxy and Content Management is back and you need it...**

Internal & External Defenses in Depth



IBM Internet Security Systems

Ahead of the Threat™

PROFESSIONAL SECURITY SERVICES

- Information Security Assessments
- Network Penetration Testing
- Compliance & Certification Services
(PCI, ISO1779 SOX, HIPAA+)
- Incident Response Planning
- Emergency Response Services
- Forensic & Legal eDiscovery Services
- Security Education & Training



X-FORCE SECURITY RESEARCH & DEVELOPMENT

Global Threat Operations Centers monitor Internet threats 24x7x365, advising the U.S. government, military, industry & clients.

200+ full time analysts perform primary research & consolidate industry-wide research into the largest, most authoritative database of security vulnerabilities.

Continually update ISS products with new protection engines & updates.

X-Force Daily Threat Analysis Service
X-Force Research Subscription

PROVENTIA SECURITY PROTECTION PRODUCTS

Integrated Management System

- Vulnerability Management
- Network Access Control
- Network Intrusion Prevention
- Network Behavior Analysis/Anomaly Detection
- Server Intrusion Prevention
- Desktop/Laptop Protection

**May be managed & monitored by ISS
Security Operations Centers**

SECURITY MANAGEMENT & COMPLIANCE PRODUCTS

- Security Event & Information Management
- Security Log Archival Service
- Email & Instant Messaging Archival Service
- Email & Web Filtering Service
- Compliance Reporting
- Identity Management
- Access Management
- Single Sign On

MULTI-VENDOR

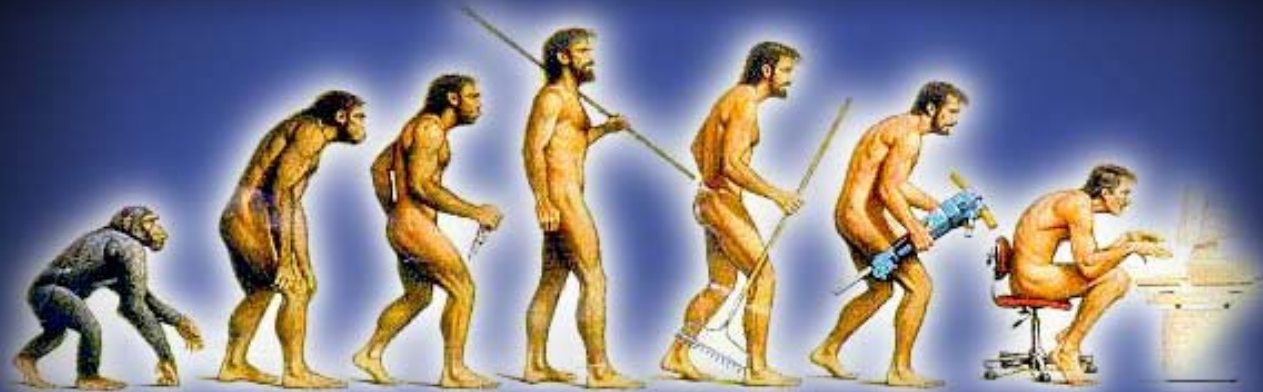
SECURITY OPERATIONS SERVICES

Guaranteed Protection

- 24x7 Management & Monitoring of Firewalls, VPNs, Intrusion Prevention, Multifunction Appliances, Servers, Desktops +)
- Global Network of SAS70 Certified Security Operations Centers
- 100% Certified Security Analysts
- Client Advocacy Program
- Industry Leading Service Level Agreements

Summary: 3 Reasons You Need to Evolve Your Security

- 1) The Security Landscape has forever Changed from “Glory” to “Profit”
- 2) Bots, Malcode ,Ransomware & Rootkits *undermine* “Legacy Security Solution”
- 3) The Enemy don't *want* to be detected...
- 4) You will have a data breach; “Are you ready?”



proventia[®]management

SiteProtector™

Unified Enterprise Security
Console for all products



**Enterprise Protection Products
(Appliances and Agents)**

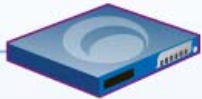
proventia[®]network
Enterprise Scanner



*All based upon the Proventia
Unified Protection Architecture (UPA)*

proventia[®]network

Protection Appliances



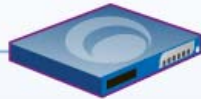
Proventia Network MFS

M50, M30, M10
"All-in-One" Protection Appliance

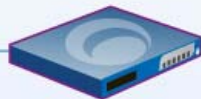
- IDS/IPS
- FW / VPN
- AntiVirus (signature & behavioral)
- AntiSpam
- Web Filter
- Spyware

proventia[®]network

Protection Appliances



Proventia ADS Series –
"Anomaly/Behavioral" Protection and
Network Visibility Appliances



Proventia Network IPS

Preemptive Security for Enterprise Networks
GX4002, GX4004, GX5008, GX5108
G400, G2000

proventia[®]server

Protection Agent



Proventia Server

"Multi-layered" Protection Agent
– Windows
– Linux

RealSecure Server Sensor

– Windows
– Solaris
– AIX
– HP-UX

proventia[®]desktop

Protection Agent



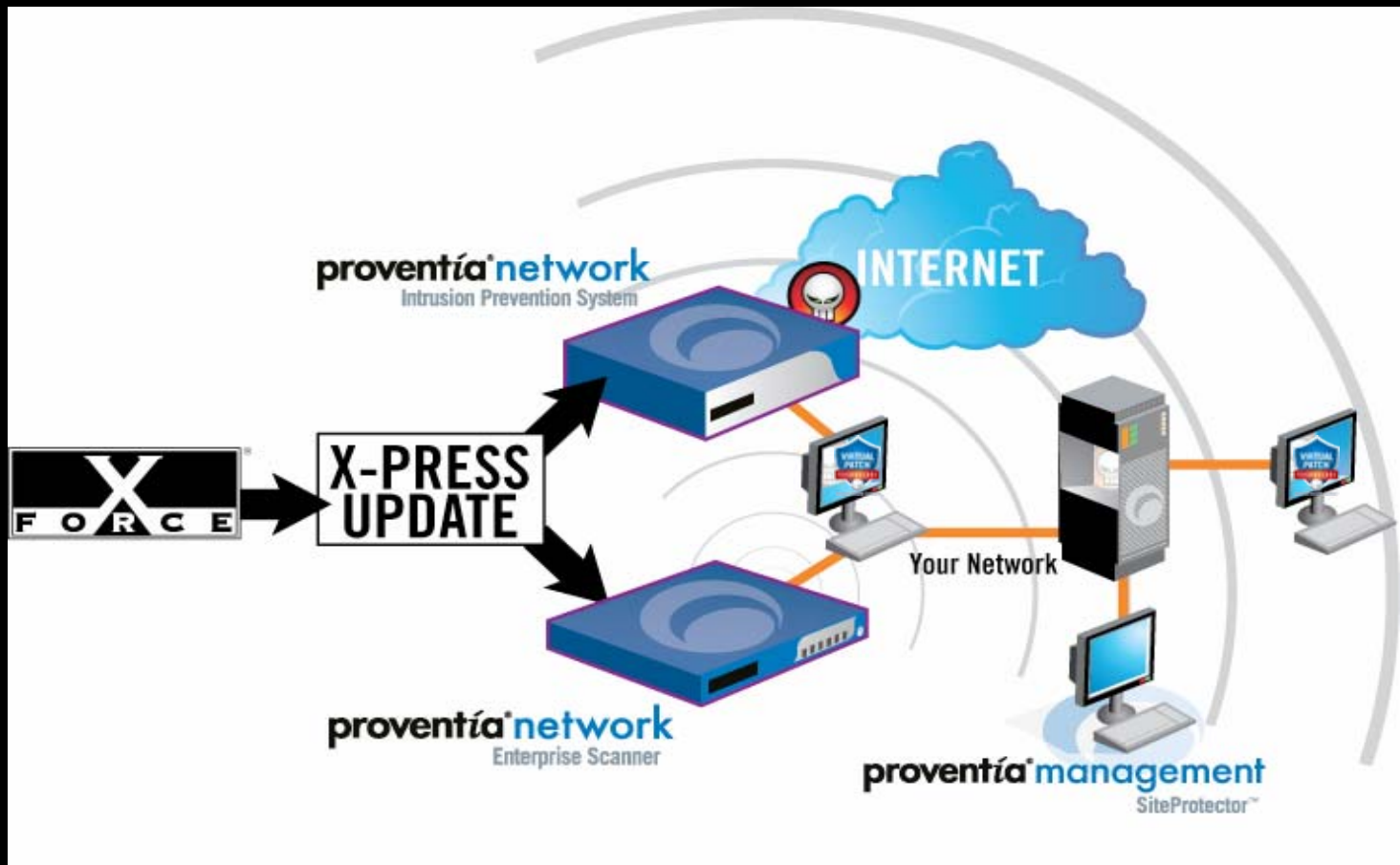
Proventia Desktop

"All-in-One" Protection Agent

- Firewall
- Virus Prevention System
- Intrusion Prevention
- VPN Enforcer
- Buffer Overflow Protection

IBM Enterprise Scanner Vulnerability Management

- Provides traditional **Patch and Protect** process for removing vulnerabilities
- Works with IPS to **Scan and Block** malicious and unwanted traffic and allow time for any vendor supplied patches to be applied



The Core of ISS' IPS

Protocol Analysis Module (PAM)

Port Assignment

Heuristics

Port Following

Protocol Tunneling

Protocol Analysis

RFC Compliance

TCP Reassembly

Flow Reassembly

Statistical Analysis

Pattern Matching

Protocol Recognition

More than 148 Protocols –
Including VoIP Protocols

Traffic Analysis

Vulnerability Based Protection
Driven by More Than 2,000
Algorithms



Internet Security Systems®

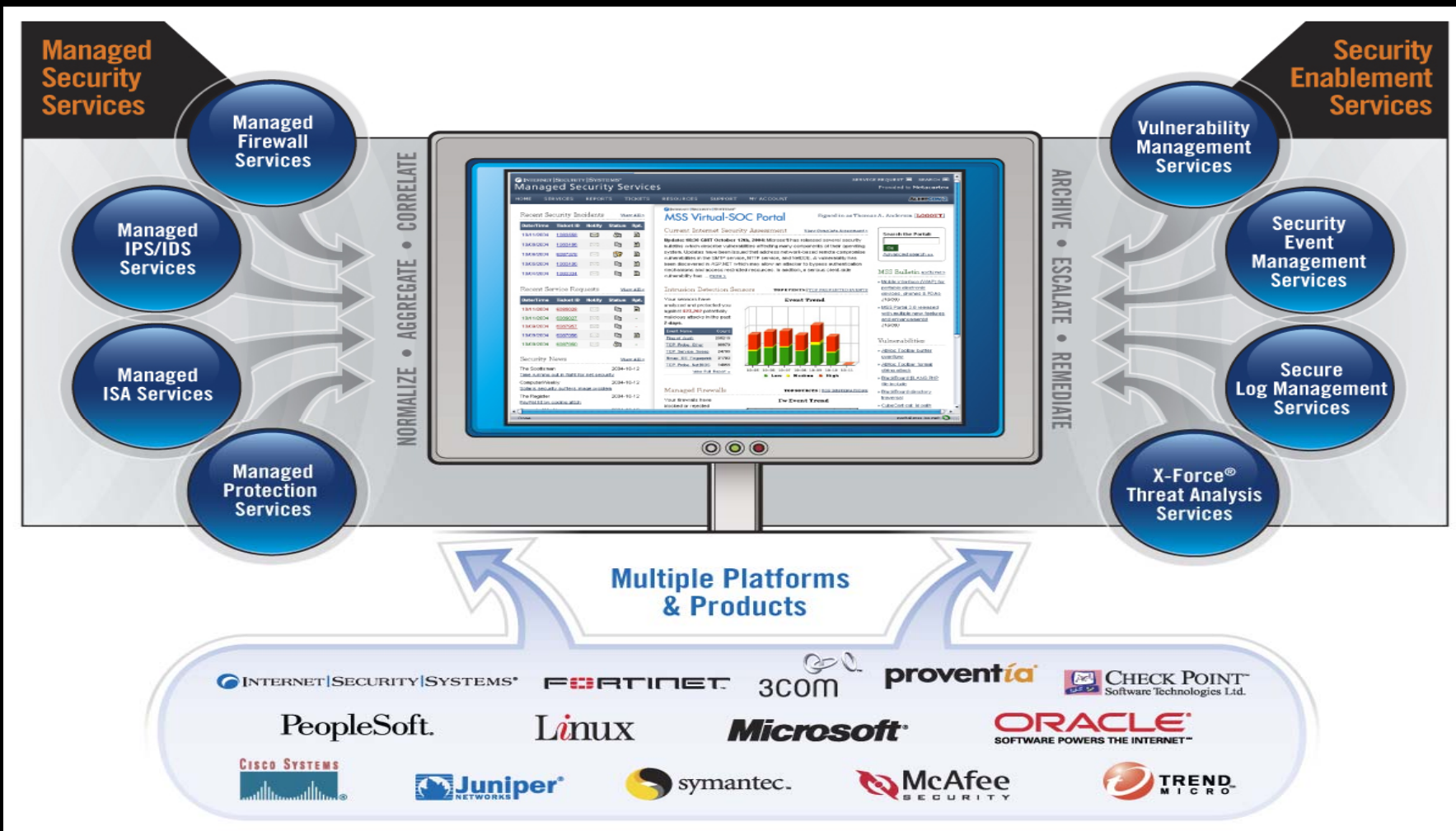


IBM Proventia Host Based Security



The Next Generation of MSS

The Virtual "Security Operations Center"





IBM Global Services

Thank you

Sean Brantley
Security Sales Specialist Florida

(386) 562-2740

sbrantle@us.ibm.com



IBM Internet Security Systems®
Ahead of the threat.™