

# IT Security in 2009

---

**Where are we now...**

**...Where are we going?**

**Jim Hietala**

VP, Security

CISSP, GSEC

[j.hietala@opengroup.org](mailto:j.hietala@opengroup.org)

# Agenda

---

- ❑ Threats, vulnerabilities, attack types
- ❑ Business requirements affecting security
- ❑ Technological shifts
- ❑ Work to be done
- ❑ Open Group security activities
  - Security Forum
  - Jericho Forum
  - Real Time and Embedded Systems Forum

# IT Security Failures Abound...

## Insiders


- Symantec survey, 79% take data upon leaving company
- Mass propagating worms and viruses
- Targeted attacks at high-value targets
- Class action suits in large breaches



Magazine The Week Blogs Special Reports Subs

VA agrees to pay \$20M in laptop theft case

By Mary Mosquera Jan 28, 2009



Home News Travel Money Sports Life Tech

Money » Personal Finance Taxes Retirement Mortgage/CD Rates Stock/Fund/ETF

GET A QUOTE: Enter symbol(s) or Keywords GO DJIA 7,928.70 -4.06 NASDAQ 1,545.90 +4

## Hackers breach Heartland Payment credit card system

By Byron Acohido, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.



cnet news

Latest News Crave Webware Business Tech Green Tech Wire

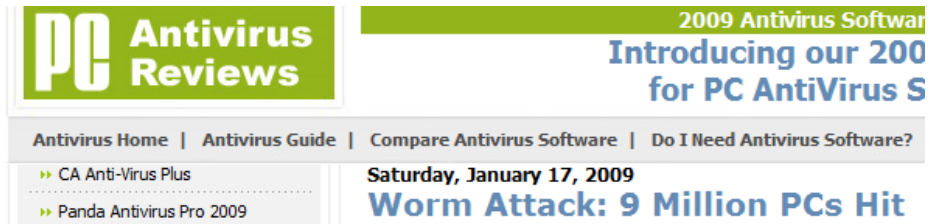
Home > News > Security

### Security

February 5, 2009 5:14 PM PST

## FBI: Cloned debit cards used in worldwide scheme

by Elinor Mills 4 comments



2009 Antivirus Software

## Introducing our 200 for PC AntiVirus S

Antivirus Home | Antivirus Guide | Compare Antivirus Software | Do I Need Antivirus Software?

- CA Anti-Virus Plus
- Panda Antivirus Pro 2009

Saturday, January 17, 2009

## Worm Attack: 9 Million PCs Hit

THE Open GROUP

Making standards work®

# Vulnerabilities

---

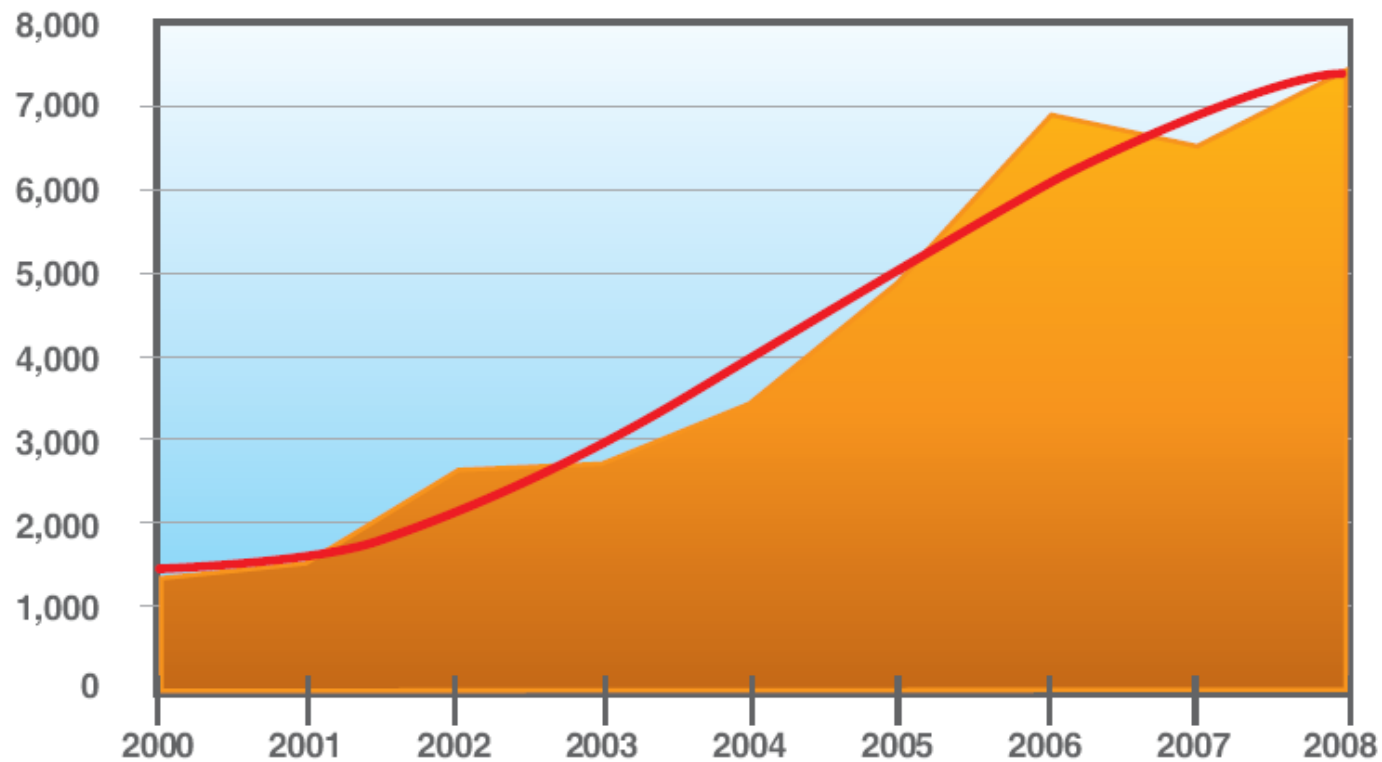
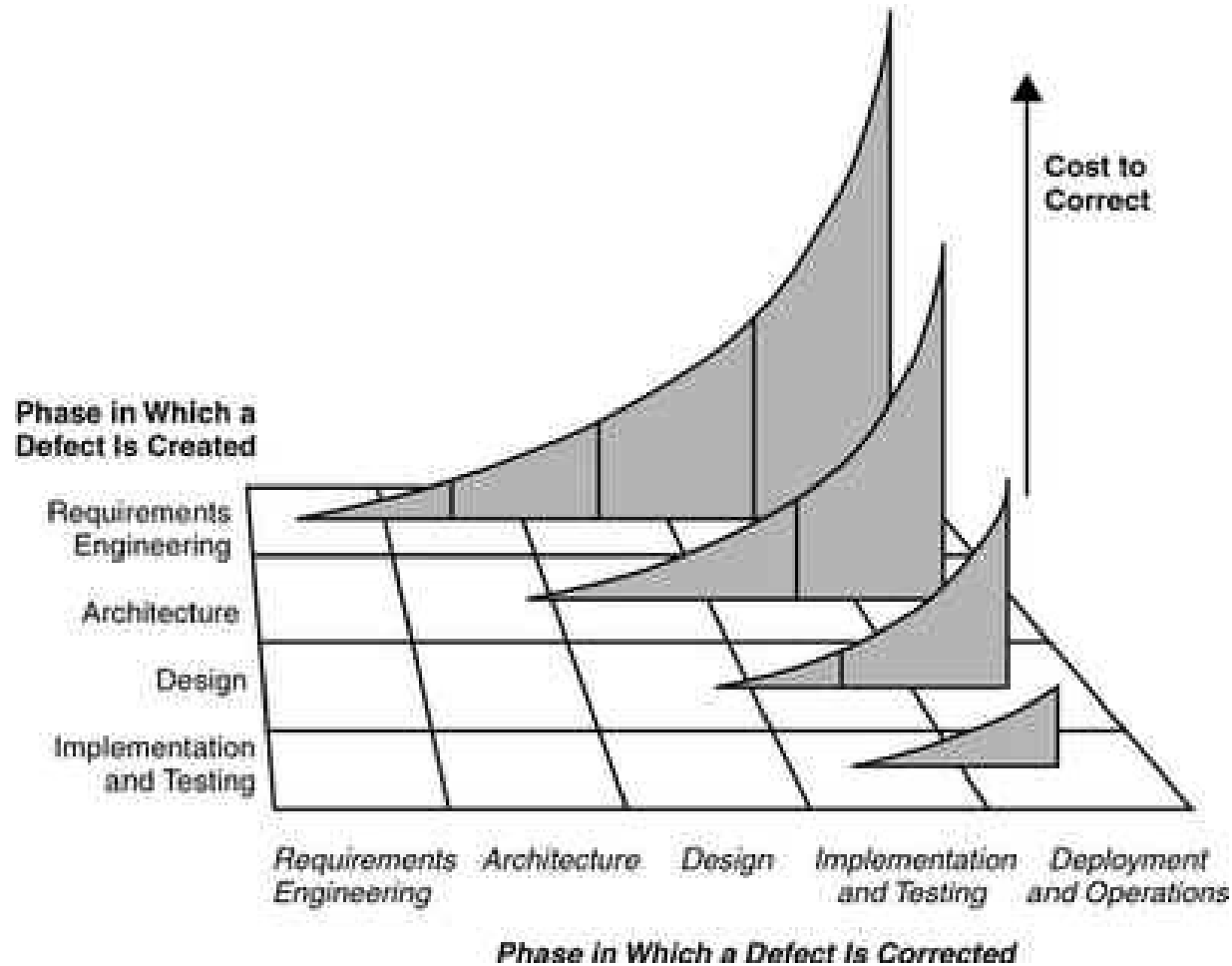


Figure 8: Vulnerability Disclosures, 2000 – 2008

IBM ISS Xforce 2008 Annual Report

# Creating Secure Software

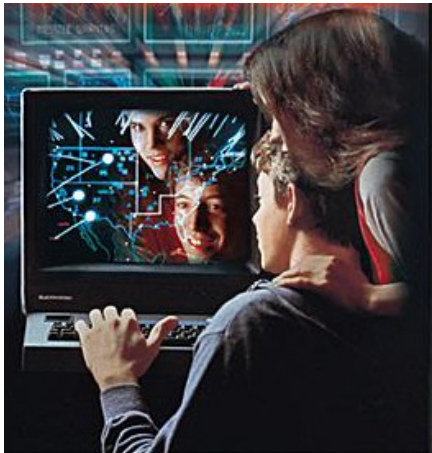
---



# Threats & Attackers, Then and Now

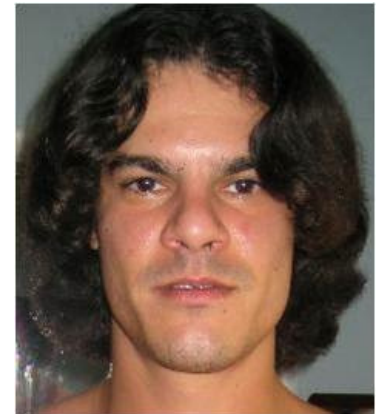
---

## □ Then:



## □ Now:

- Profit motivated criminals
- Global, leverage freely available tools
- Sophisticated attackers and attacks



### Russian Business Network

From Wikipedia, the free encyclopedia

The **Russian Business Network** (commonly abbreviated as **RBN**) is a multi-faceted [cybercrime](#) organization, cases monopolizing personal identity theft for resale. It is the originator of [MPack](#) and an alleged operator of the [RBN](#), which is notorious for its hosting of illegal and dubious businesses, originated as an [Internet service provider](#) [phishing](#), [spam](#), and [malware](#) distribution physically based in [St. Petersburg, Russia](#). By 2007, it developed [phishing](#) techniques in many countries to provide a method for [organized crime](#) to target victims internationally.<sup>[4]</sup>

# Endpoint Attacks

---

- ❑ Spam is increasingly used as an attack vector, to drive victims to websites that will drop malware on victim's PC
  - Multiple objectives, including phishing attacks to extract confidential account information, financial fraud, trojan and sniffer programs, and to add to botnets and use as spam delivery agents

# DDoS Attacks

---

- ❑ Use Botnets of compromised PC's to flood traffic at target websites
  - Politically motivated attacks against Estonia, Georgia, US sites
- ❑ Extortion/protection against e-commerce sites, including onsite gambling operations, with DDoS as the threat

SECURITY  
**darkREADING**  
Protect The Business  Enable Access

ATTACKS / BREACHES

VULNERABILITIES

APPLICATION

SECURITY MANAGEMENT

STORAGE SECURITY

ENCRYPT

## Denial-Of-Service Attacks Hard To Kill

**While tweets went silent last week, hundreds of other DDoS attacks were under way around the globe -- and several more powerful ones**

Aug 10, 2009 | 06:12 PM

By Kelly Jackson Higgins  
*DarkReading*

Turns out Twitter, Facebook, and LiveJournal weren't the only sites hit hard by major distributed denial-of-service (DDoS) attacks late last week, and their attacks definitely weren't the biggest: More than 770 different DDoSes were spotted across the globe last Thursday.

One DDoS attack that took out a 3G mobile operator in Asia's Web portal was a powerful, 30 gigabit-per-second one, according to Craig Labovitz, chief scientist at Arbor Networks, who has been [tracking](#) the recent trends in DDoS attacks. The 30-Gbps DDoS was unusually potent; most attacks average about 1 Gbps or less, according to Arbor.

"There are hundreds of DDoS attacks any given day," Labovitz says.

**THE Open GROUP**  
Making standards work®



# Website Attacks

---

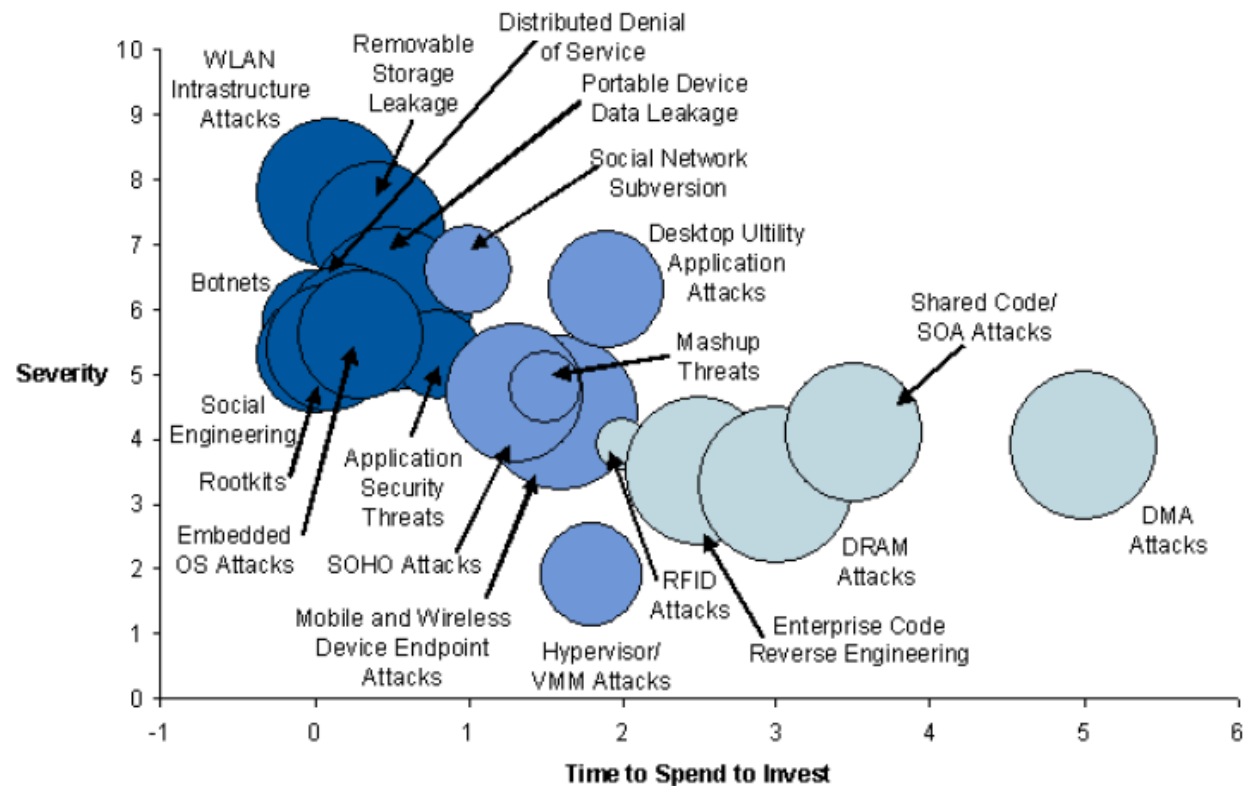


- ❑ Retail example: Heartland, TJX, 7-eleven, Hannaford, Dave & Buster's
- ❑ Impact: 130M+ credit card records stolen, extensive credit card fraud, massive costs to banks to reissue cards
- ❑ Attack Methodology:
  - They identify Web sites that are vulnerable to SQL injection. They appear to target MSSQL only.
  - They use "xp\_cmdshell", an extended procedure installed by default on MSSQL, to download their hacker tools to the compromised MSSQL server.
  - They obtain valid Windows credentials by using fgdump or a similar tool.
  - They install network "sniffers" to identify card data and systems involved in processing credit card transactions.
  - They install backdoors that "beacon" periodically to their command and control servers, allowing surreptitious access to the compromised networks.
  - They target databases, Hardware Security Modules (HSMs), and processing applications in an effort to obtain credit card data or brute-force ATM PINs.
  - They use WinRAR to compress the information they pilfer from the compromised networks.

# Emerging Threats



Figure 1. Summary Threat Timeline



Source: Gartner (August 2008)

# Cyber Security

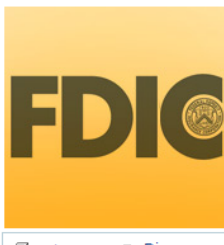


## Bank Information Security Articles

### FDIC Warns of Online Fraud Against Banks, Small Businesses

#### Alert Cites Increase in ACH, Wire Transfer Fraud

August 26, 2009 - Linda McGlasson, Managing Editor



Online crime is increasingly hitting small and mid-size companies in the U.S., draining those entities' bank accounts through fraudulent transfers. The problem has gotten so bad that a financial services group recently sent out a warning about the trend, and the Federal Deposit Insurance Corporation (FDIC) issued an alert today.

"In the past six months, financial institutions, security companies, the media and law enforcement agencies

InfoWorld INFOWORLD CHANNELS Application

## SECURITY CENTRAL

Sign in or Register

News Blogs Discussions White Papers Webcasts Podcasts



AUGUST 28, 2009

### We're losing the war on cybercrime

While we chase after two-bit malicious hackers, cybercrime syndicates remain untouchable

Sign In | Register Now

## The Washington Post

TODAY'S NEWSPAPER  
Subscribe | PostPoints

Advertisement

What's in it for your family? Repower America  
It's time to get real.  
ROLL OVER to learn more.  
Paid for by the Alliance for Climate Protection

NEWS POLITICS OPINIONS BUSINESS LOCAL SPORTS ARTS & LIVING GOING OUT GUIDE JOBS CARS REAL ESTATE RENTALS CLASSIFIEDS

SEARCH:  washingtonpost.com Web : Results by Google | Search Archives

washingtonpost.com > Technology > Tech Policy

» THIS STORY: READ + | Comments

### European Cyber-Gangs Target Small U.S. Firms, Group Says

By [Brian Krebs](#)  
Washington Post Staff Writer  
Tuesday, August 25, 2009

Organized cyber-gangs in Eastern Europe are increasingly preying on small and mid-size companies in the United States, setting off a multimillion-dollar online crime wave that has begun to worry the nation's largest financial institutions.

TOOLBOX  
Resize Print E-mail  
Yahoo! Buzz  
Constant Contact TRY EMAIL MARKETING FREE FOR 60 DAYS!

COMMENT

Advertisement > Your Ad Here

Making fast, faster.  
First and only wireless 4G network from a national carrier.



# Cyber Warfare

---

- ❑ 2007 attacks on Estonia, by Russian hackers
- ❑ Continuous attacks on US government institutions, attacks originating in China
- ❑ Recent DDoS attacks on US and UK government agencies and suppliers, attributed to N. Korea

# New Technologies Causing Security Concerns

---

- ❑ SOA
- ❑ Web 2.0
- ❑ Consumerization of IT, mobile devices
- ❑ Virtualization
- ❑ Cloud computing

# Cloud Security and Risks to CIA

## Confidentiality...Integrity... Availability?

Social site [Ma.gnolia.com](http://Ma.gnolia.com) suffered catastrophic failure (1/09), rendering all users' data irrecoverable. Backup facility wasn't setup properly, was never tested.



Home | Security | Mobile & Telecoms | Internet | Server |

■ Salesforce.com outage darkens cloud computing

**An outage disrupts thousands of the software-as-a-service vendor's customers just as businesses get back to work after the New Year.**  
By Miya Knights, 8 Jan 2009 at 11:49



**Salesforce.com** suffered a major outage earlier this week, leaving thousands of its customers unable to access applications.



### S3 Outage Highlights Fragility of Web Services

Om Malik | Sunday, July 20, 2008 | 7:46 PM PT | 69 comments



**Updated with Statement from Amazon:** Amazon's S3 cloud storage service went offline this morning for an extended period of time — the second big outage at the service this year. In February, Amazon suffered a major outage that knocked many of its customers offline.



**Something is technically wrong.**

Thanks for noticing—we're going to fix it up and have things back to normal soon.

Powered By  
**InformationWeek**  
BUSINESS TECHNOLOGY  
NETWORK



Practical Technology Expertise for Growing Companies

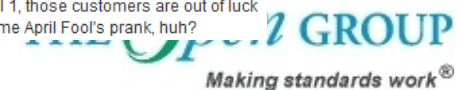


### The Demise Of Coghead: Collateral Damage When The Cloud Goes Poof

Posted by Fredric Paul Friday, Feb 20, 2009, 08:19 PM ET

The demise of Platform as a Service (PaaS) vendor Coghead is being described as a "debacle" and a "disaster" for the small and midsize companies who were using applications built on Coghead's cloud-based platform. Here's the story from the trenches.

This week's [failure of Coghead](#) has sent [shockwaves](#) through the cloud-computing community. Because although [SAP has agreed to buy the failed company's assets](#), it has not agreed to support Coghead customers. As of April 1, those customers are out of luck and must find a new way to run their applications. Some April Fool's prank, huh?



# Web Apps and Web 2.0 Risk

---

- ❑ Web application security issues (XSS, SQL injection, CSRF, and others)
- ❑ Web 2.0 technologies (AJAX, REST, JSON, RSS), security vulnerabilities categories include:
  - Insufficient authentication controls
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Phishing
  - Information Leakage
  - Injection Flaws
  - Information integrity
  - Insufficient anti-automation

# Business Requirements Affecting Security

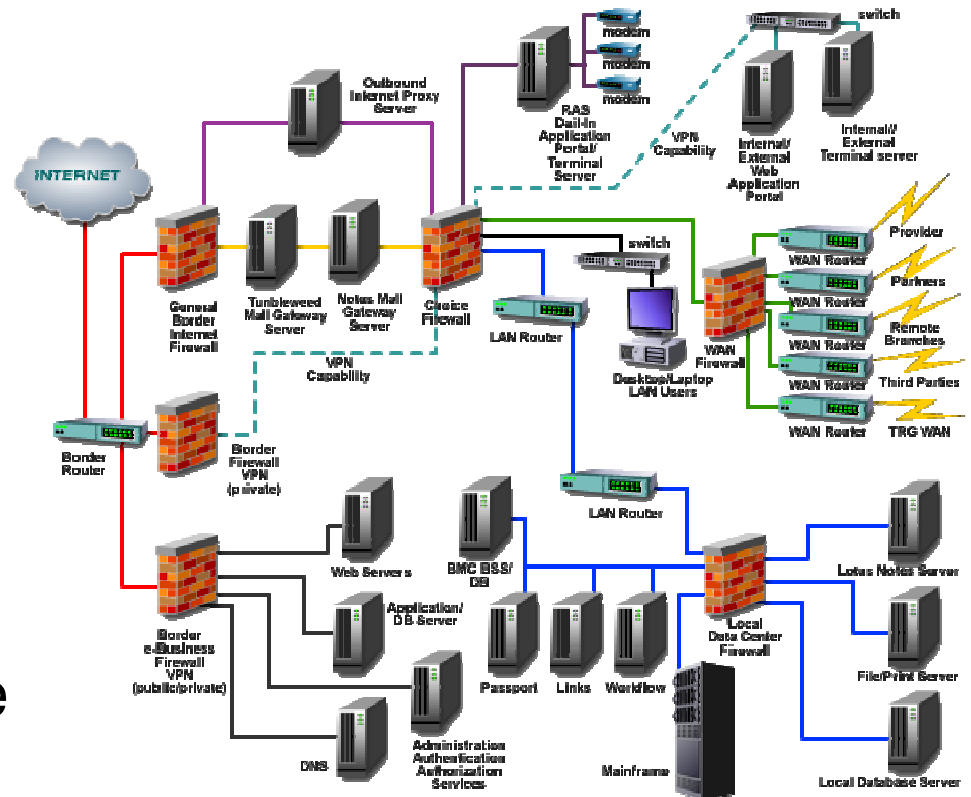
---

- ❑ Greater access for non-employees
- ❑ E-commerce
- ❑ Collaboration
- ❑ Downsizing
- ❑ Outsourcing



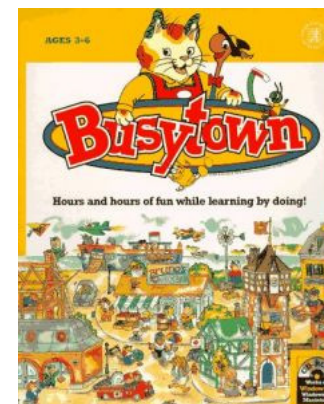
# Traditional Security Architectures

- ❑ Status quo is location-centric security
- ❑ Protection placed at the edge or perimeter of the network
- ❑ New threats and threat vectors = new security point solutions
- ❑ Consequence is that there are now over 1,000 vendors of security point solutions...



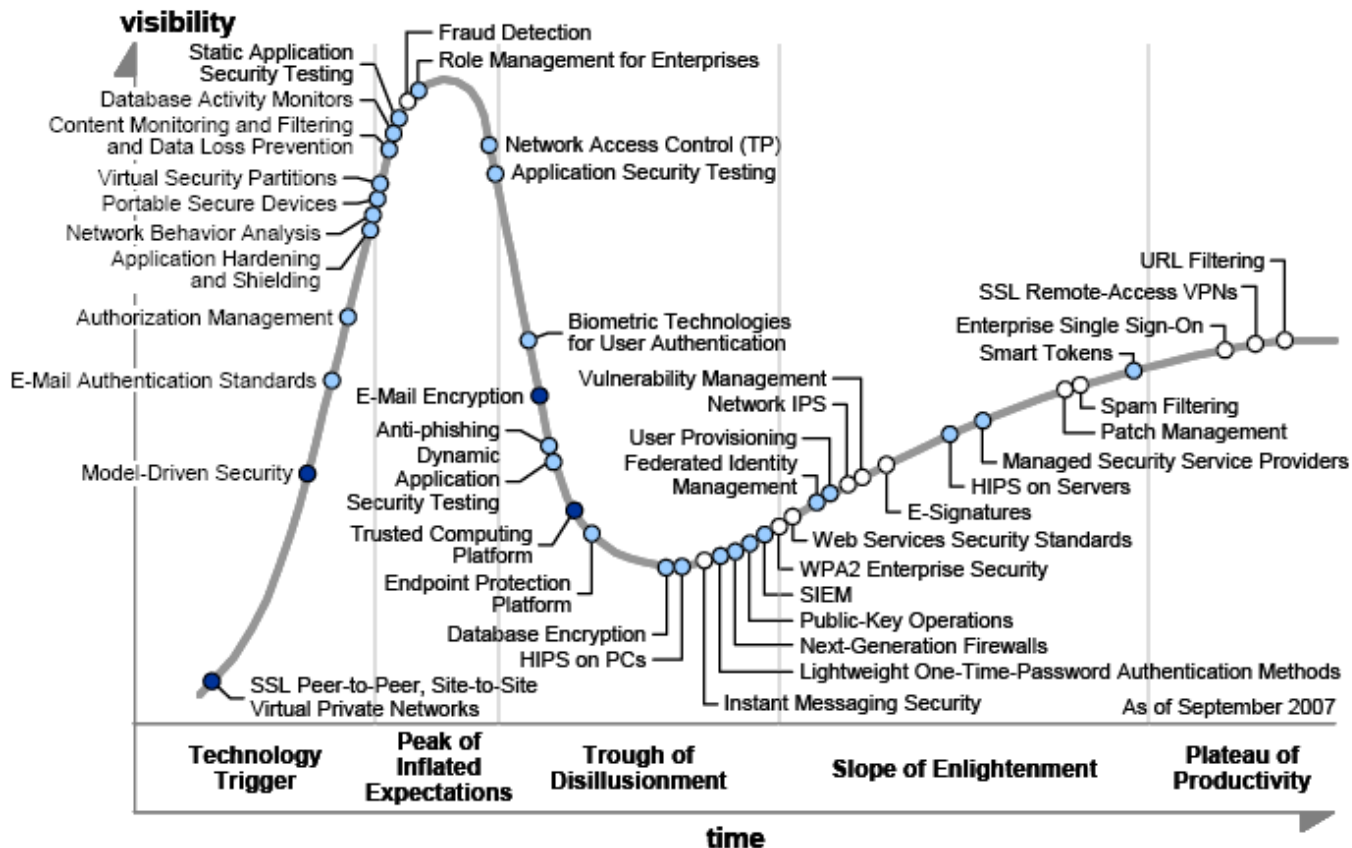
# Security Industry Response to Application Development Innovation...

	Developers	Security
1995	CGI, PERL	Network firewalls, SSL
1997	ASP, JSP	Network firewalls, SSL
1998	EJB, J2EE, DCOM	Network firewalls, SSL
1999	SOAP, XML	Network firewalls, SSL
2001	Rest, SOA	Network firewalls, SSL
2003	Web 2.0	Network firewalls, SSL
2007	Cloud Computing	Network firewalls, SSL



# Narrow Problem View, Narrow Solution Scope

Figure 1. Hype Cycle for Information Security, 2007



Years to mainstream adoption:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

Source: Gartner (September 2007)

**GROUP**

Making standards work®

# Security Industry: Part of the Problem

---

- ❑ The “security industry” is part of the problem
- ❑ 800 vendors, 30 to 50 different product niches
- ❑ Vendors claiming to be “silver bullets” or “magic elixirs” for various problems
- ❑ Little independent information on actual control effectiveness



# How Bad are Things, Really?

---



# Some Positive Developments...

---

- ❑ Breach notification laws (45+ states) have heightened interest in and funding for IT security initiatives
- ❑ PCI DSS is maligned by many, but has undeniably “raised the floor” for IT security among retailers
- ❑ Microsoft’s security focus and SDL are improving the security of their Os’es and other applications
- ❑ In the US there is starting to be recognition that there’s a government role to be played in improving IT security, 5 bills being worked involving IT security

# General Issues

---

- ❑ Too much data, not enough usable information
  - No actuarial information on security attacks, incidents
  - No independent information about controls effectiveness
- ❑ Debate over risk-based vs. best practices approach
- ❑ Incentives for secure software products aren't there
  - ❑ *"take your best shot with a prototype, immediately get it to market, iterate quickly"*  
Guy Kawasaki, The Art of the Start
- ❑ SW license agreements are purely one sided
  - *"By clicking the "I agree" button..you are agreeing to act as crash test dummies without any chance of holding the software manufacturer to account for injuries,*

# Specific Areas for Improvement

---

- ❑ Training software developers in secure coding, SDL, critical to developing secure web apps
- ❑ Prioritizing, selecting appropriate security controls- need more information about which security controls work, which don't
- ❑ Making information security management less art and more science, maturity models & metrics
- ❑ Tying information security to business objectives
- ❑ Easing the burden of risk, compliance, and audit



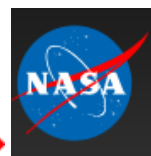
# Security Forum Vision & Mission

---

- The Open Group: Boundaryless Information Flow, achieved through global interoperability in a secure, reliable and timely manner
- The Open Group Security Forum: To facilitate the rapid development of secure architectures supporting boundaryless information flow through:
  - Development of industry standards, either independently or through co-operation (adopt, adapt, publish)
  - Developing guides, business rationales & scenarios, use cases
  - Developing reference and common system architectures, and support services



Dept. Work & Pensions, UK



# Audit, Compliance, Risk Initiatives

---

- ❑ Audit & Logging: Update to XDAS standard, aligning with MITRE CEE
- ❑ ACEML compliance standard, to automate compliance configuration and reporting
- ❑ Risk Management
  - Risk Taxonomy Standard, and Risk Assessment Methodologies – Technical Guide published
  - Cookbooks for use of Taxonomy Standard with COSO, ISO, Octave, and other frameworks – in process

# Architecture Initiatives

---

- ❑ Collaboration Oriented Architecture Reference Architecture in TOGAF
- ❑ Enterprise Security Architecture
  - Updating the NAC Enterprise Security Architecture document

# Other Initiatives...

---

- ❑ Trust Framework
  - New project targeting how to architect for managing trust , includes components on Information Classification, Business Impact Levels, Impact Sensitivity, Control Stratification
- ❑ SOA Security Guide
  - Joint work with SOA Forum, producing a technical guide to securing SOA

# Jericho Forum

---

- ❑ Thought leadership around de-perimeterization, guidance as to what to do about it
- ❑ Publications:
  - Commandments, position papers, Collaboration Oriented Architecture Framework, Cloud Cube Model
- ❑ New Mission/Vision:
  - Secure Collaboration in Cloud Computing
- ❑ New projects:
  - COA (Security) Reference Architecture for TOGAF, COA Framework standard, Cloud Use Cases: business scenarios
  - “Commandments” Self Assessment Scheme
  - Security requirements in Cloud Computing
  - Identity & Access Management in de-perimeterized environments
- ❑ New Liaison – Cloud Security Alliance
  - [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)

# Some Members of Jericho



<http://www.jerichoforum.org/>

# Real Time and Embedded Systems Forum Security Activities

---

- ❑ **Secure Operating Systems**
  - **Multiple Independent Level of Security (MILS)**
  - **Significant MILS work ongoing in the Real Time Forum to remove barriers to adoption, and accelerate progress**
- ❑ **Software assurance activities**

# Summary

---

- ❑ IT security is undergoing a profound transformation in threats, business drivers, and consequently in security architectures
  - Moving away from perimeter-based security models towards information-centric security
- ❑ Customers and vendors need help in sorting out what this shift means, and what to do about it
- ❑ The Open Group (Security Forum, Jericho Forum, and Real Time & Embedded Systems Forum) develops standards, frameworks, and guides that educate, inform, and accelerate the market for secure IT systems that deliver information-centric security
- ❑ We encourage your participation in this critical work



# Resources

---

- ❑ Recommended IT Security Reading:
  - Geekonomics, The Real Cost of Insecure Software, David Rice
- ❑ Security Forum: [www.opengroup.org/security](http://www.opengroup.org/security)
- ❑ Jericho Forum: [www.opengroup.org/jericho](http://www.opengroup.org/jericho)
- ❑ Real Time & Embedded Systems Forum: [www.opengroup.org/rtforum/](http://www.opengroup.org/rtforum/)
- ❑ Risk Taxonomy Standard: <http://www.opengroup.org/bookstore/catalog/c081.htm>
- ❑ Technical Guide to Risk Assessment: <http://www.opengroup.org/bookstore/catalog/g081.htm>
- ❑ ACEML draft standard information: <http://www.opengroup.org/projects/security/ace/>

# Questions?

---

**Jim Hietala, VP, Security, The Open Group**

**[Http://www.opengroup.org/security](http://www.opengroup.org/security)**

**e-mail: [j.hietala@opengroup.org](mailto:j.hietala@opengroup.org)**

**Twitter: [jim\\_hietala](https://twitter.com/jim_hietala)**