



Mitsis LLC

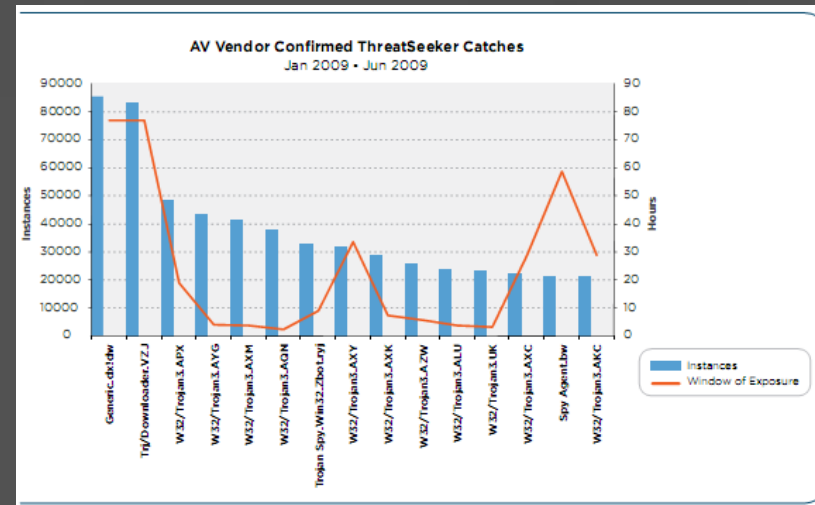
Federal Information Security Buzz

Overview

- Let's Talk Shop
 - Complementary Perspective
 - Some Helpful References
- Agenda
 - How is the Threat Looking?
 - How are We Looking?
 - What is the Strategy?
 - What Should be the Tactics?

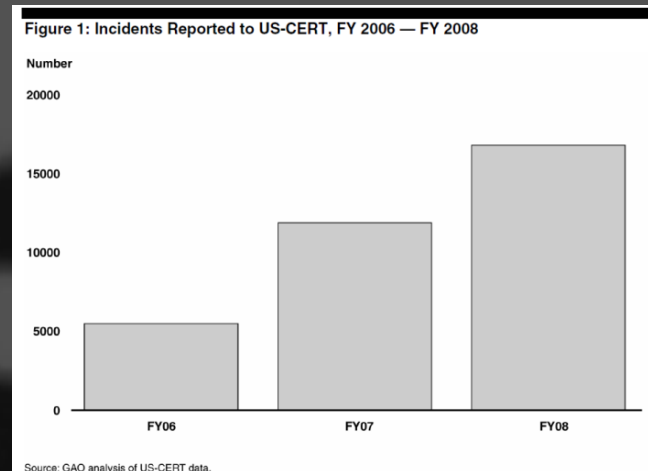
How is the Threat Looking?

- 233% growth in the number of malicious sites in the last six months and a 671% growth during the last year.
 - 77% of Web sites with malicious code are legitimate sites that have been compromised.
 - 95% of comments to blogs, chat rooms and message boards are spam or malicious.
 - 57% of data-stealing attacks are conducted over the Web.
 - 85.6% of all unwanted emails in circulation contained links to spam sites and/or malicious Web sites.



How is the Threat Looking?

- “Revenue from cybercrime has exceeded drug trafficking as the most lucrative illegal global business, reaping in more than \$1 trillion annually in illegal profits.”
 - Or not
 - <http://homelandsecuritynewswire.com/notion-cybercrime-exceeds-drug-trade-myth>
- Reported incidents at Federal agencies has more than tripled in the period 2006 – 2008.
 - See GAO Report GAO-09-701T



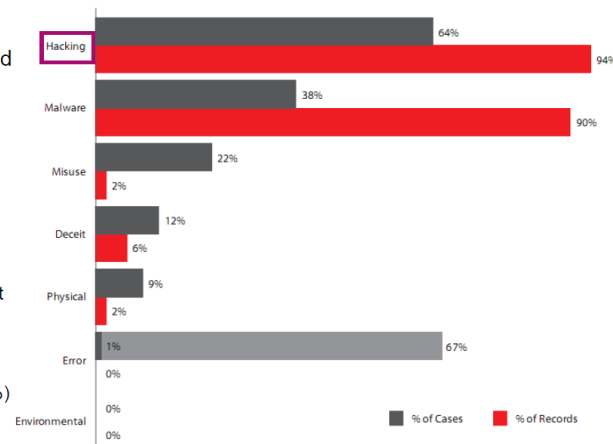
How is the Threat Looking?

- 285M records compromised in 2008
- 90+% of breached records attributed to organized crime activity
- Hacking and malware are principal threats
 - See *2009 Verizon Business' Data Breach Investigations Report*



Threats and Attacks

- Similar to previous 4 years for breach percentages
- Most breaches and records linked to Hacking & Malware
- Misuse is fairly common
 - Mostly admin abuse
- Deceit and social attacks
 - Involved a range of methods, vectors, and targets
- Physical attacks
 - Represent minority of caseload
 - Portable media in one case (but not essential to breach)
- Error is extremely common
 - Rarely the direct cause
 - Usually contributing factor (67%)



How Are We Looking?

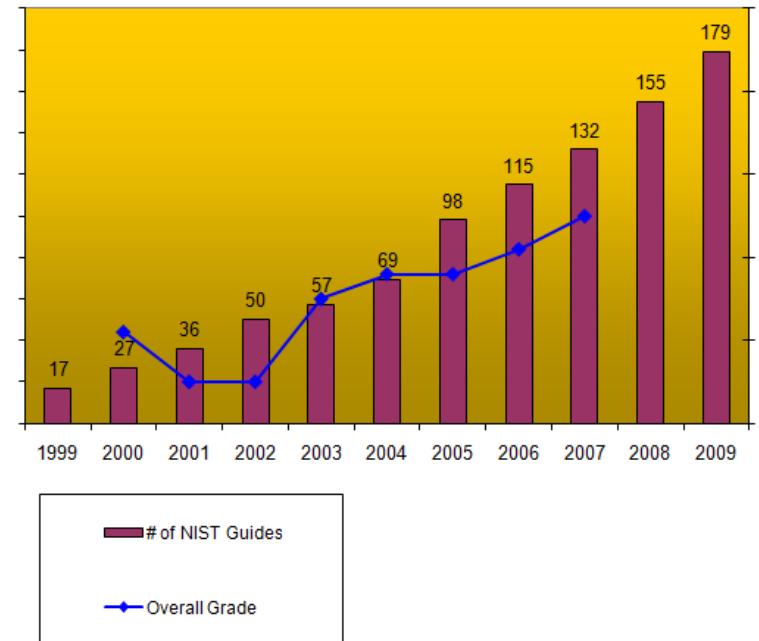
- Federal Agencies
 - \$74.2B Total IT Spending planned FY2009
 - 5.25% on IT Security (\$3.89B)



How Are We Looking?

- FISMA Report Card

| Agency | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 |
|----------------|-----------|----------|----------|----------|-----------|-----------|-----------|----------|
| SSA | B | C+ | B- | B+ | B | A+ | A | A+ |
| NSF | B- | B+ | D- | A- | C+ | A | A+ | A+ |
| Labor | F | F | C+ | B | B- | A+ | B- | D |
| NRC | | F | C | A | B+ | D- | F | F |
| EPA | D- | D+ | D- | C | B | A+ | A- | A+ |
| USAID | C- | F | F | C- | A+ | A+ | A+ | A+ |
| GSA | D- | D | D | D | C+ | A- | A | B+ |
| Education | C | F | D | C+ | C | C- | F | C- |
| Transportation | | F | F | D+ | A- | C- | B | D |
| NASA | D- | C- | D+ | D- | D- | B- | D- | C |
| OPM | F | F | F | D- | C- | A+ | A+ | A- |
| Commerce | C- | F | D+ | C- | F | D+ | F | D+ |
| State | C | D+ | F | F | D+ | F | F | C |
| SBA | F | F | F | C- | D- | C+ | B+ | B |
| Treasury | D | F | F | D | D+ | D- | F | F |
| HUD | C- | D | F | F | F | D+ | A+ | A |
| Justice | F | F | F | F | B- | D | A- | A+ |
| DoD | D+ | F | F | D | D | F | F | D- |
| VA | D | F | F | C | F | F | F | F |
| Interior | F | F | F | F | C+ | F | F | F |
| FEMA/DHS | | D | F | F | F | F | D | B+ |
| HHS | F | F | D- | F | F | F | B | B |
| Agriculture | F | F | F | F | F | F | F | F |
| Energy | | F | F | F | F | F | C- | B+ |
| Overall | D- | F | F | D | D+ | D+ | C- | C |



How Are We Looking?

- “FISMA compliance grades may have improved over the years, but there does not seem to be a correlation between an agency’s FISMA compliance and the state of its cyber security posture.”
 - May 5, 2009, Testimony by Liesyl Franz, Vice President of Information Security and Global Public Policy TechAmerica before House Subcommittee on Management, Organization, and Procurement.
- “Should we believe the Federal Computer Security Report Card?”,
 - http://www.relevanttechnologies.com/fedcomp_120109.asp

How Are We Looking?

- Reports

GAO

United States Government Accountability Office

Testimony

Before the Subcommittee on Federal Financial Management,
Government Information, Federal Services, and
International Security, Committee on Homeland Security

For Release on Delivery
Expected at 2:30 p.m. EDT
Wednesday, March 12, 2008

GAO

United States Government Accountability Office

Report to Congressional Committees

July 2009

INFORMATION SECURITY

Agencies Continue to
Report Progress, but
Need to Mitigate
Persistent Weaknesses

GAO-08-571T

GAO-09-546



Gartner

Research

Publication Date: 9 July 2009

ID Number: G00169719

'North Korean' Attacks Show Lack of Basic Internet Protections

John Pescatore

A highly publicized series of "cyberattacks" really just represents business as usual on the Internet. Businesses and government agencies that depend of the Internet should already have protections against such attacks.

How Are We Looking?

- “However, recent successful breaches at the Federal Aviation Administration and at the vendor that hosts USAjobs.gov demonstrate that the current state of information security at Federal agencies is not what the American people have the right to expect. The Federal Information Security Management Act (FISMA) has been in place for 7 years. It has raised the level of awareness in the agencies and in the country at large, but we are not where we need to be.”



May 19, 2009, Testimony by Vivek Kundra, Federal CIO, before House Subcommittee on Management, Organization, and Procurement.

What Is The Strategy?

- “Security Cyberspace for the 44th Presidency”, Dec 2008
 - Center for Strategic and International Studies
 - Comprehensive National Security Strategy for Cyberspace
 - Organizing for Cybersecurity
 - Rebuilding Partnership with the Private Sector
 - Regulate for Cybersecurity
 - Identity Management for Cybersecurity
 - Modernize Authorities
 - Build for the Future
 - “My Administration is committed to treating our digital infrastructure as a strategic national asset”
 - 10/1/2009, President Barack Obama

What Is The Strategy?

- National Asset



Rep Issa, (R-CA), House Subcommittee on Management, Organization, and Procurement , May 5, 2009

“But if we do not begin working smarter, using techniques to attack our enemies”

“to get to the hacker before the hacker gets to us...”

“to change, or at least, attempt to change international law...”

“...as aggressive acts of cyberwar...”

What is the Strategy?

- National Asset
 - Cybersecurity Coordination and Awareness Act (Bill)
 - NIST gaining responsibility for coordinating US Government efforts with international organizations on cybersecurity standards.
 - http://science.house.gov/legislation/leg_highlights_detail.aspx?NewsID=2674

What is the Strategy?

- The Cloud
 - “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”
 - <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>

What is the Strategy?

- The Cloud
 - Why

General Security Advantages

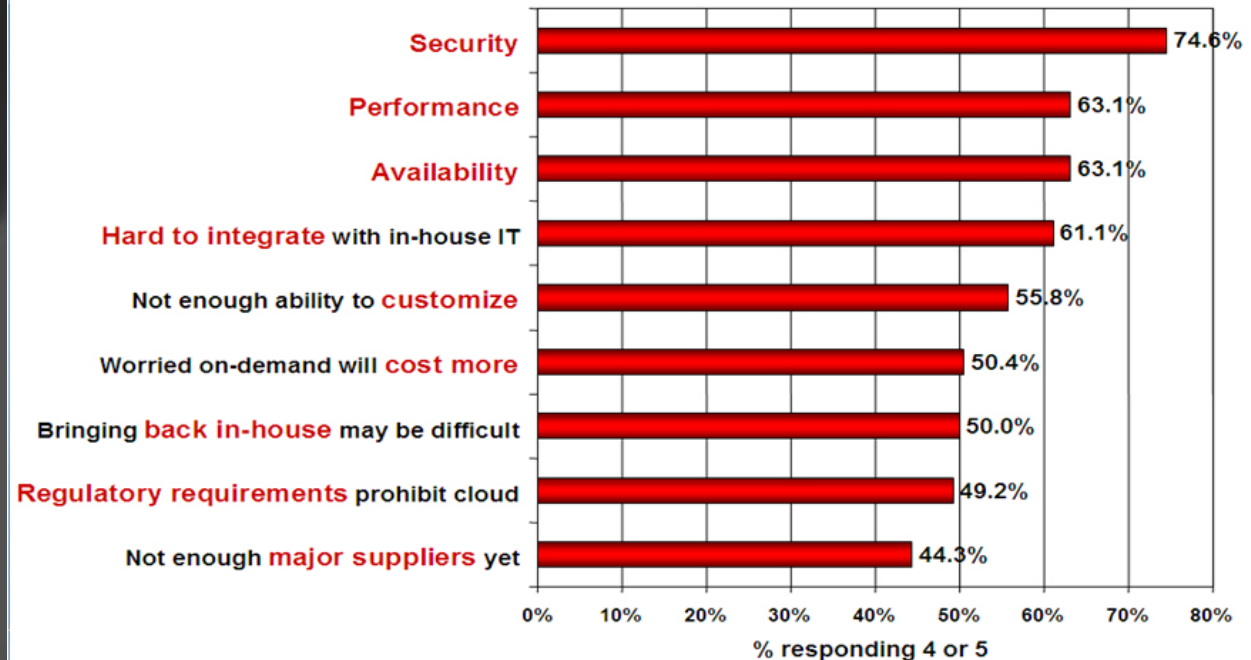


- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

What is the Strategy?

- The Cloud
 - Why Not?

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

What is the Strategy?

- The Cloud
 - Why Not

General Security Challenges



- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control

What Should be the Tactics?

- Consensus Audit Guidelines (CAG)
 - Short-hand, practical priorities for prioritizing security investments against threats
 - Consortium effort among DoD, Federal, and other computer security organizations.
 - The US State Department, under CISO John Streufert, has already demonstrated more than 80% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls.
 - <http://www.sans.org/critical-security-controls/guidelines.php>

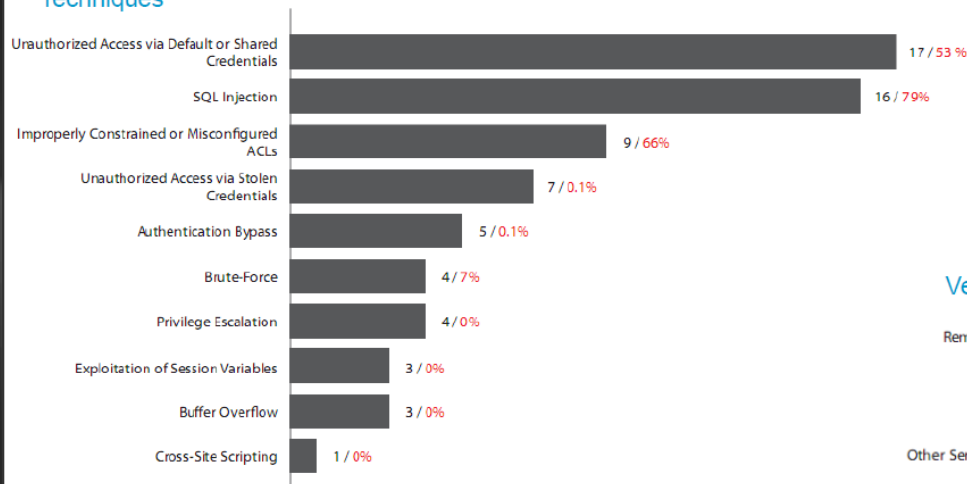
What Should be the Tactics?



Breakdown of Hacking (64% of breaches)

- Default credentials and SQL injection most common
- Often specifically targeting database-attached environments
- Few and old vulnerabilities exploited
- Web Apps & Remote Access are main vectors

Techniques

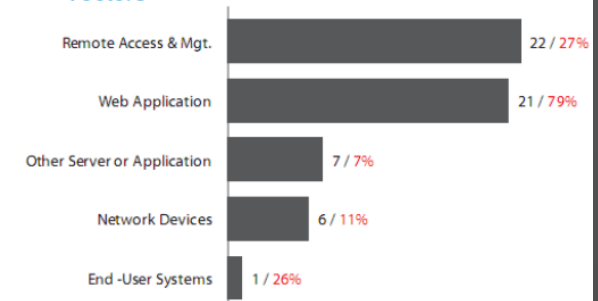


Vulnerability Exploits

Table 2. Patch availability at time of breach

| | |
|-------------------|---|
| Less than 1 month | 0 |
| 1 to 3 months | 0 |
| 3 to 6 months | 0 |
| 6 to 12 months | 1 |
| More than 1 year | 5 |

Vectors



- Open web application security project (OWASP)
- http://www.owasp.org/index.php/Main_Page

What Should be the Tactics?

- Mobile data commensurate with harm



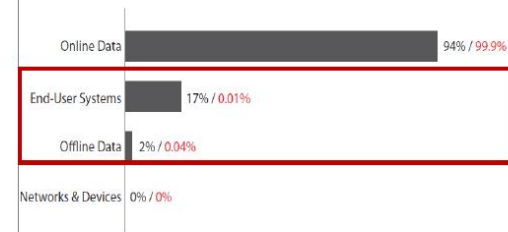
Breakdown of Hacking (Database Servers)

Database servers = 75% of all compromised records.

| Asset | Asset Group | % of Breaches | % of Records |
|-----------------------------------|-----------------|---------------|--------------|
| POS system | Online Data | 32% | 6% |
| Database server | Online Data | 30% | 75% |
| Application server | Online Data | 12% | 19% |
| Web server | Online Data | 10% | 0.004% |
| File server | Online Data | 8% | 0.1% |
| Public kiosk system | Online Data | 2% | 0.4% |
| Authentication / Directory server | Online Data | 2% | 0.1% |
| Backup tapes | Offline Data | 1% | 0.04% |
| Documents | Offline Data | 1% | 0.000% |
| Workstation | End-User System | 8% | 0.01% |
| Laptop | End-User System | 4% | 0.000% |
| PIN Entry Device | End-User System | 2% | 0.004% |

Laptops and backup tapes account for only <0.05% of breached records

Figure 25. Asset classes by percent of breaches (black) and records (red)



“Although much angst and security funding is given to **offline data, mobile devices, and end-user systems**, these assets are simply **not a major point of compromise.**”

Good webinar summary including Christopher Novak (Verizon Business) at :
<https://www.techwebonlineevents.com/ars/eventregistration.do?mode=eventreg&F=1001859&K=6TW>

What Should be the Tactics?

- Work your logs
 - “What I often see is the scenario that people are not implementing the right technology or are not implementing the technology properly, or don’t have the resources there to back up the technology”
 - Christopher Novak, Managing Principal & Founding Member, Verizon Business’ Investigative Response Team

Figure 32. Breach discovery methods by percent of breaches

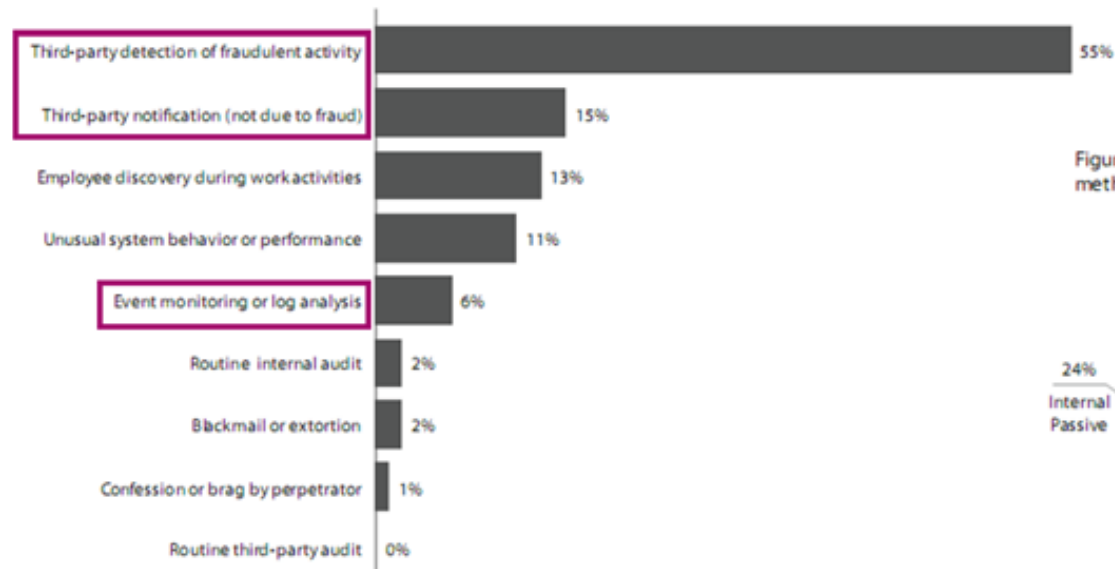
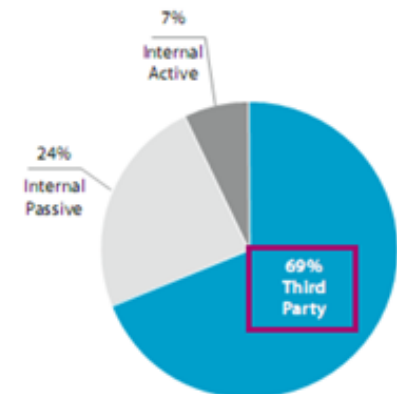


Figure 33. Breach discovery methods, simplified



What Should be the Tactics?

- In- / Out- source
 - Most organizations cannot cover all necessary technologies and control families with 5% of IT staff
 - IT staff is 3-4% of organization

| | | |
|---------------|------------|-----------|
| 10,000 | 350 | 17 |
| 3,000 | 95 | 5 |

- Contracts – Identify
 - access requirements to operational / investigative / auditing information
 - Seek to preserve provider confidentiality (third-party)
 - service levels including rule / profile changes
 - multi-org OLAs
 - FIPS 200 levels



Always Happy to Rumininate

Joel Hurford

CISSP, PMP, ITIL, MCSE, MCSA, CCNA, VCP

Joel.Hurford@mitsis.com