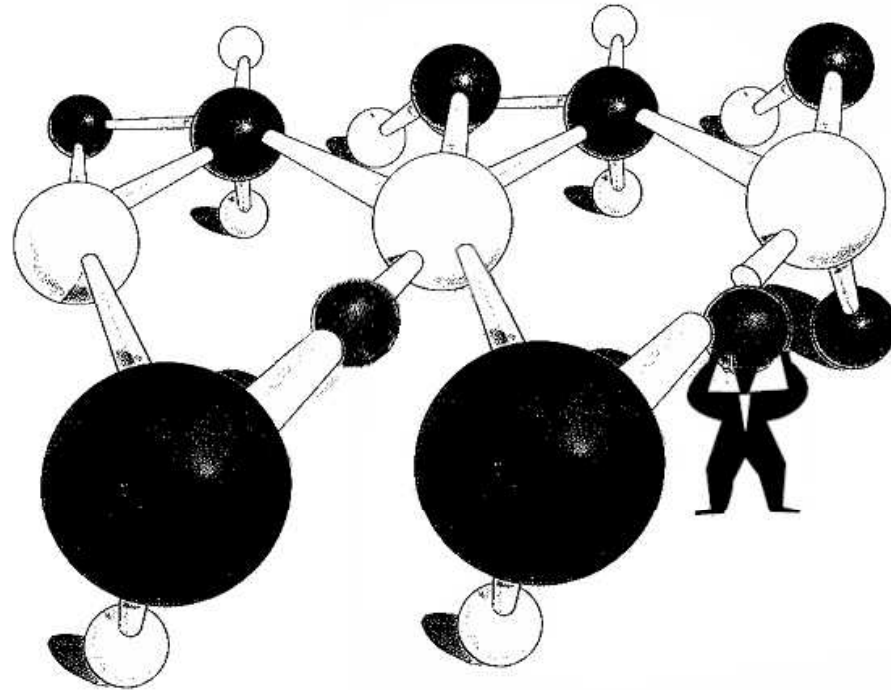


On Agility and Governance in Security Systems



CSER

Invited Talk

070314

Rick Dove

Stevens Institute of Technology

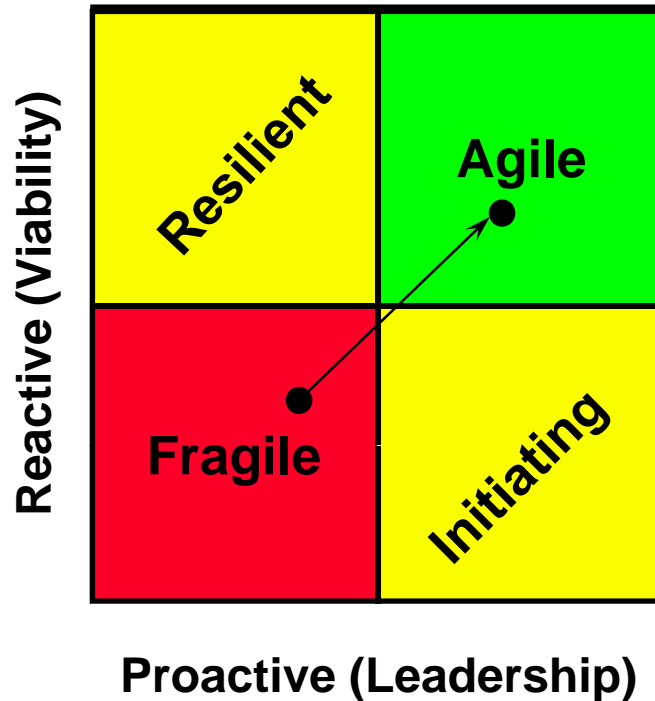
Governance

... is essentially about ensuring that business is conducted properly. It is less about overt control and strict adherence to rules, and more about guidance and effective and equitable usage of resources to ensure sustainability of an organization's strategic objectives. [The Open Group]

... is a program that makes sure that people do what's "right." ... A governance program is implemented using policies, processes, metrics, and organization.

[The Burton Group]

Agility



... is
the ability to
respond effectively
at *all* times,
reactively *and* proactively,
within mission.

The ability to survive and thrive
in an unpredictable and uncertain environment

Class 1 Agile Systems are Reconfigurable

Useful Metaphor: Plug-and-Play – Drag-and-Drop

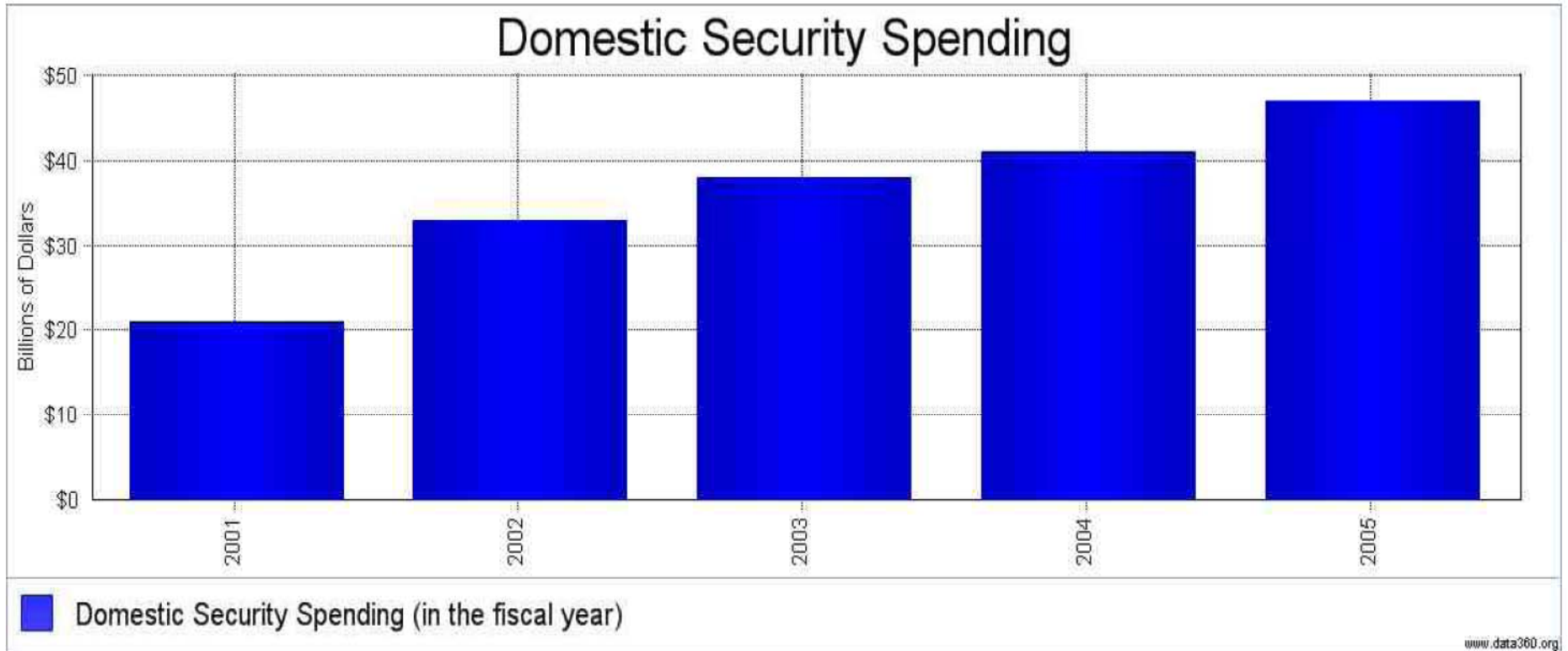
Class 2 Agile Systems are Reconfiguring

Useful Metaphor: Complex Adaptive Systems

They Share 10 Common Design Principles

1. Evolving **Framework** Standards
2. Encapsulated **Modules**
3. Plug Compatibility
4. Facilitated Module Reuse
5. Module Redundancy/Diversity
6. Elastic Capacity
7. Distributed Control & Information
8. Deferred Commitment / Late Binding
9. Loosely Coupled Flat Interaction
10. Self Organization

The Facts



Security Spending Exceeds 7% of IT Budgets

ITA Premium: Trends & Predictions, Nov 15, 2006

Security is a ubiquitous topic with IT managers today. This note helps build understanding of how much of the IT budget is being allocated to security and further divides this expenditure into technology acquisition (i.e. purchases) and operational expenditures. Key findings include:

Security is growing as a percent of IT budget and it presently accounts for more than 7% of all IT spending.

Total security spending by IT managers in the **U.S. is modeled at \$61 billion.**

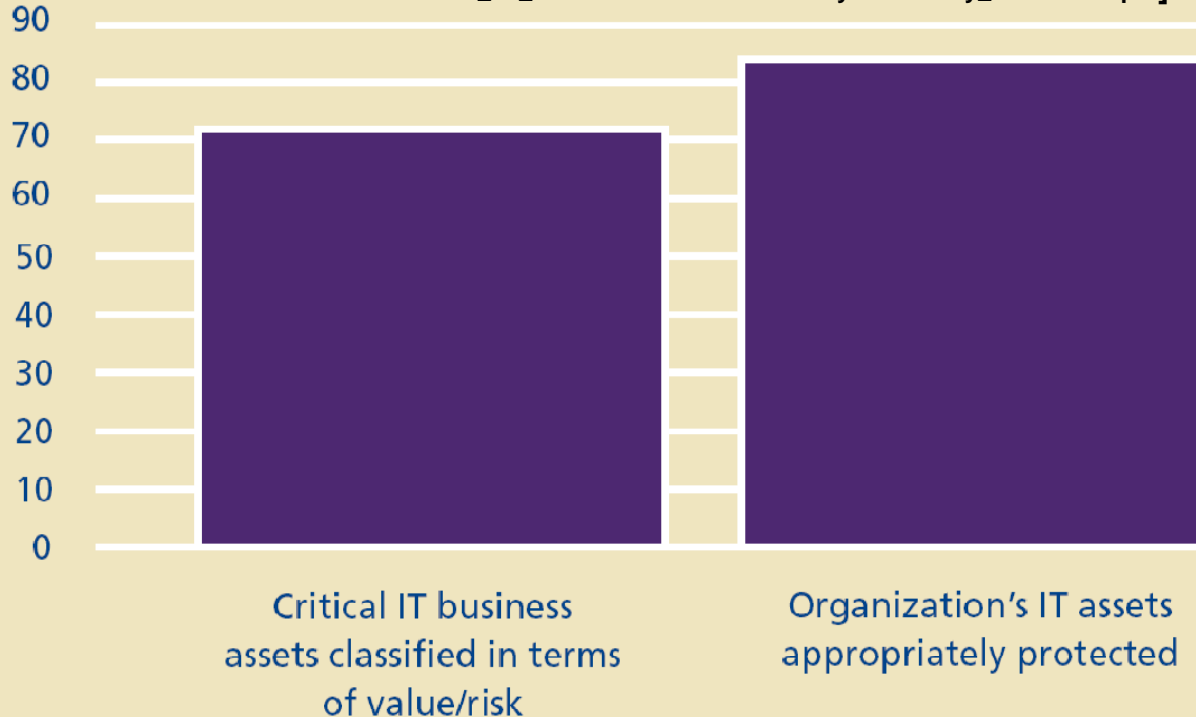
Between \$21 and \$27 billion is spent on technology acquisition (i.e. purchases) and the remainder on operations (i.e. mainly staffing).

<http://www.infotech.com/Research/Notes/ITAP/SecuritySpendingExceeds7PercentofITBudgets.aspx?PublicationNumber=%7B8CDEBC81-E22D-4074-AFBB-786B954B2309%7D&SubCenter={0CE23E8A-D3BE-40F0-8E78-32B6309142DA}>

Managing and protection of IT assets

[Deloitte 2006 Global Security Survey

www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf]



External breaches included:

- Viruses/worms – 63%.
- Phishing/pharming – 51%.
- Spyware/malware – 48%.
- Social engineering – 25%.
- Brand hijacking – 15%.
- Hacking – 10%.
- Denial of service – 10%.
- Zombie networks – 7%.
- Website defacement – 4%.
- Web application breach – 3%.
- Wireless network breach – 1%.
- Online extortion – 1%.
- Other external breach – 5%.

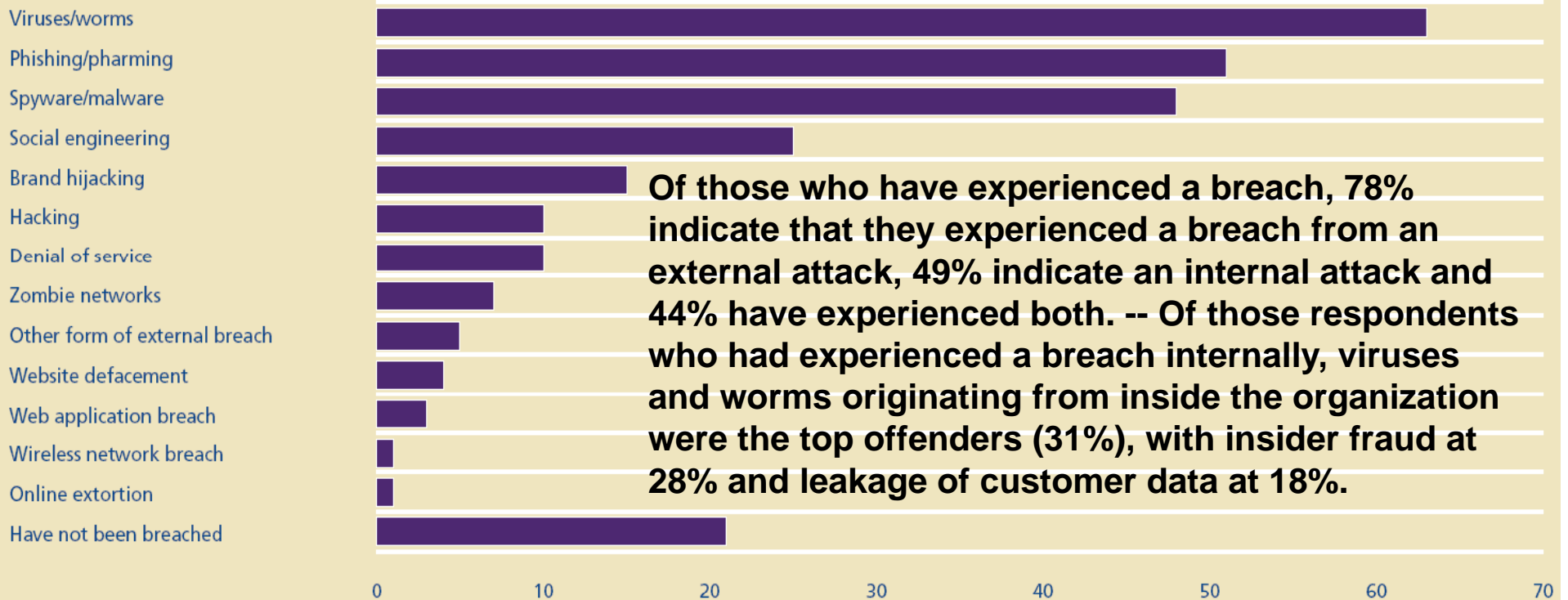
It has been said that there is no future without risk. New technology ranks right up there with one of those undertakings of greatest risk. The increasing demand for mobility, agility and interoperability being placed on the IT and security functions has led to exponential growth in a variety of communication mediums, all of which open the door to new kinds of risk.

In 2004, 83% of respondents indicated that they had experienced some form of successful breach, either internally or externally. ... the percentage this year [2006] remains relatively unchanged (82%) from 2004.

External breaches over the past 12 months

[Deloitte 2006 Global Security Survey

www.deloitte.com/dtt/cda/doc/content/dtt_fsi_2006%20Global%20Security%20Survey_2006-06-13.pdf]

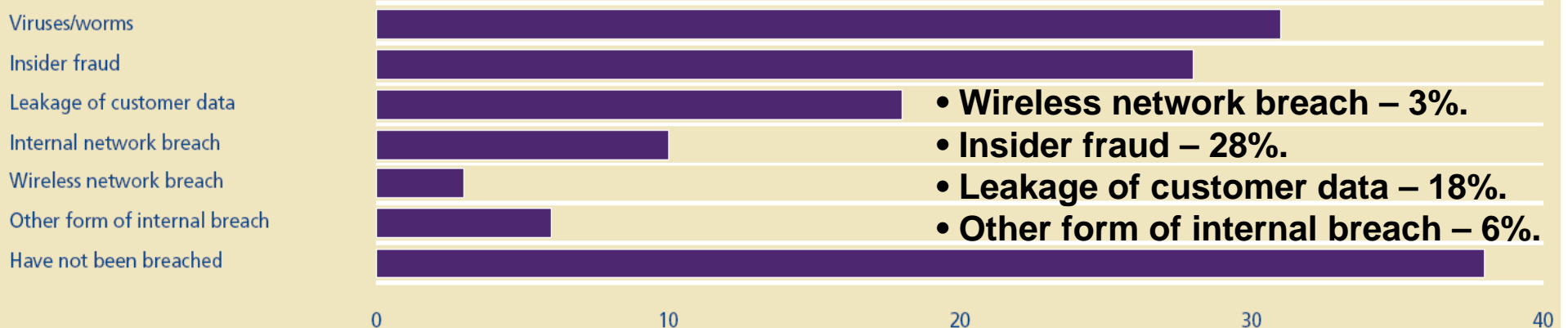


Of those who have experienced a breach, 78% indicate that they experienced a breach from an external attack, 49% indicate an internal attack and 44% have experienced both. -- Of those respondents who had experienced a breach internally, viruses and worms originating from inside the organization were the top offenders (31%), with insider fraud at 28% and leakage of customer data at 18%.

Internal breaches included:

- Viruses/worms – 31%.
- Internal network breach – 10%.
- Wireless network breach – 3%.
- Insider fraud – 28%.
- Leakage of customer data – 18%.
- Other form of internal breach – 6%.

Internal breaches over the past 12 months



Two-Thirds of Companies Lose Data Six Times a Year

SANS NewsBites

March 7, 2007

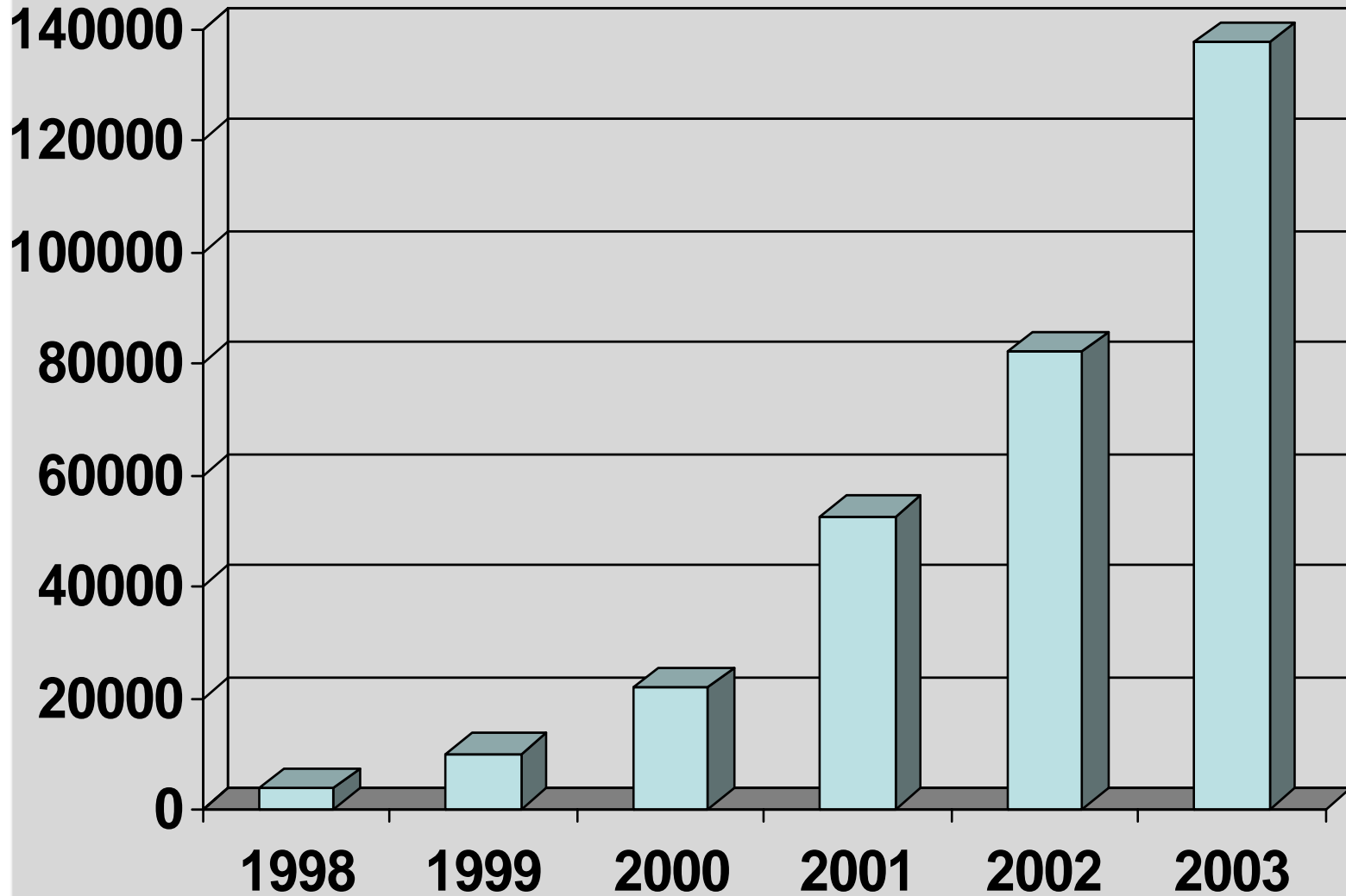
Sixty-eight percent of companies surveyed by the **IT Policy Compliance Group** said they experience data loss or theft six times a year; 20 percent say they lose data at least 22 times a year. Just 12 percent of companies report losing data less than twice a year. The **top reasons the companies gave for data loss are user error, policy violations**, and Internet threats. The ways in which data were lost include lost devices, email and other electronic communications, and software applications.

http://www.eweek.com/print_article2/0,1217,a=202593,00.asp

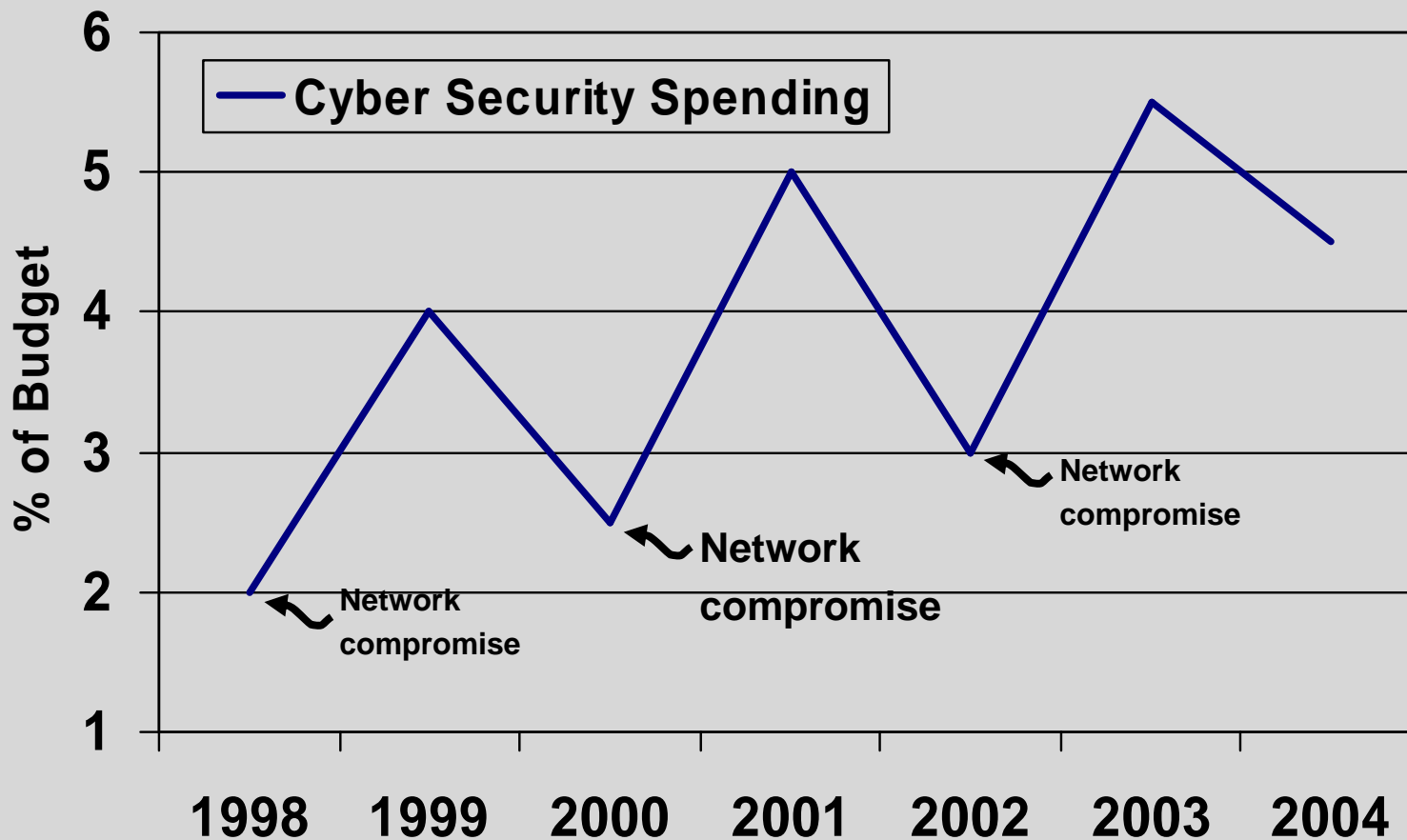
[Editor's Note (Schultz): The VA is slowly but surely doing better when it comes to information security, even though this organization has had to learn the hard way. My only concern is that the VA's approach has been to put new security-related policies and procedures in place, something that will do some amount of good, but that does not address the real root cause of the problems the VA has had--**lack of senior management governance and oversight.**]

Computer Security Incidents

From (US CERT) Computer Emergency Response Team statistics



The Reactionary Approach



IBM Internet Security Systems Report

SANS NewsBites

1 February 2007

IBM Internet Security Systems (ISS) released highlights of its 2006 security statistics report on January 30. Among their predictions for security trends 2007: Internet Explorer (IE) will continue to provide a trove of vulnerabilities, browser attacks will increase and more spam will be image-based. In addition, close to 90 percent of new vulnerabilities this year will be remotely exploitable. The report also predicts that **malware purveyors will organize themselves into more efficient networks, resulting in the development of "exploits-as-a-service" industry, and the rise of customized attacks.**

http://www.theregister.co.uk/2007/02/01/windows_vista_security/print.html

<http://www.itnews.com.au/newsstory.aspx?ClanID=45136>

http://www.eweek.com/print_article2/0,1217,a=199933,00.asp

http://www10.mcadcafe.com/nbc/articles/view_article.php?section=CorpNews&articleid=347382

Not Just Plane Vanilla Computers

March 8, 2007 – <http://www.siliconrepublic.com/news/news.nv?storyid=single7916>

The Forum of International Irregular Network Access (FIINA) estimates that **telecoms fraud is costing companies €42bn a year and is growing at 15% a year.**

Telecoms fraud currently accounts for between 30% and 50% of European telecom firms' bad debts and the arrival of new services like Internet telephony or voice over IP (VoIP) and mobile services like 3G have led to an increase in options for hackers to get into phone systems.

Gartner Study Sees Sharp Rise in ID Theft and Associated Fraud

SANS NewsBites

March 7, 2007

A Gartner study says that fraud arising from identity theft has risen significantly since 2003. Extrapolation from gathered statistics indicates that approximately 15 million Americans dealt with fraud stemming from identity theft between the middle of 2005 and the middle of 2006. ... Gartner surveyed 5,000 US adults who use the Internet. Other findings include an increase in the average amount of money lost to fraud from US \$1,408 in 2005 to US \$3,257 in 2006. The percentage of funds recovered dropped over the same one-year period from 85 percent in 2005 to just 61 percent in 2006.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012483>

<http://www.zdnetasia.com/news/security/printfriendly.htm?AT=61994518-39000005c>

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197800774>

[Editor's Note (Ullrich): I have friends who stopped using the Internet for shopping and banking due to either experiencing or hearing about identity theft. In addition to the first-order monetary damage, ID theft causes even larger damages due to loss of trust in technology. The economic damage that could be caused by this loss of trust could easily explode unless companies and agencies responsible for protecting our data wake up and get their act together, implement meaningful two factor authentication schemes.]

RSA: Identity theft remains top consumer complaint

Internet-related complaints were up too

February 07, 2007 (IDG News Service) -- Identity theft remained top of mind among U.S. consumers last year, but complaints about Internet auction fraud dropped noticeably, according to data released Wednesday by the U.S. Federal Trade Commission (FTC).

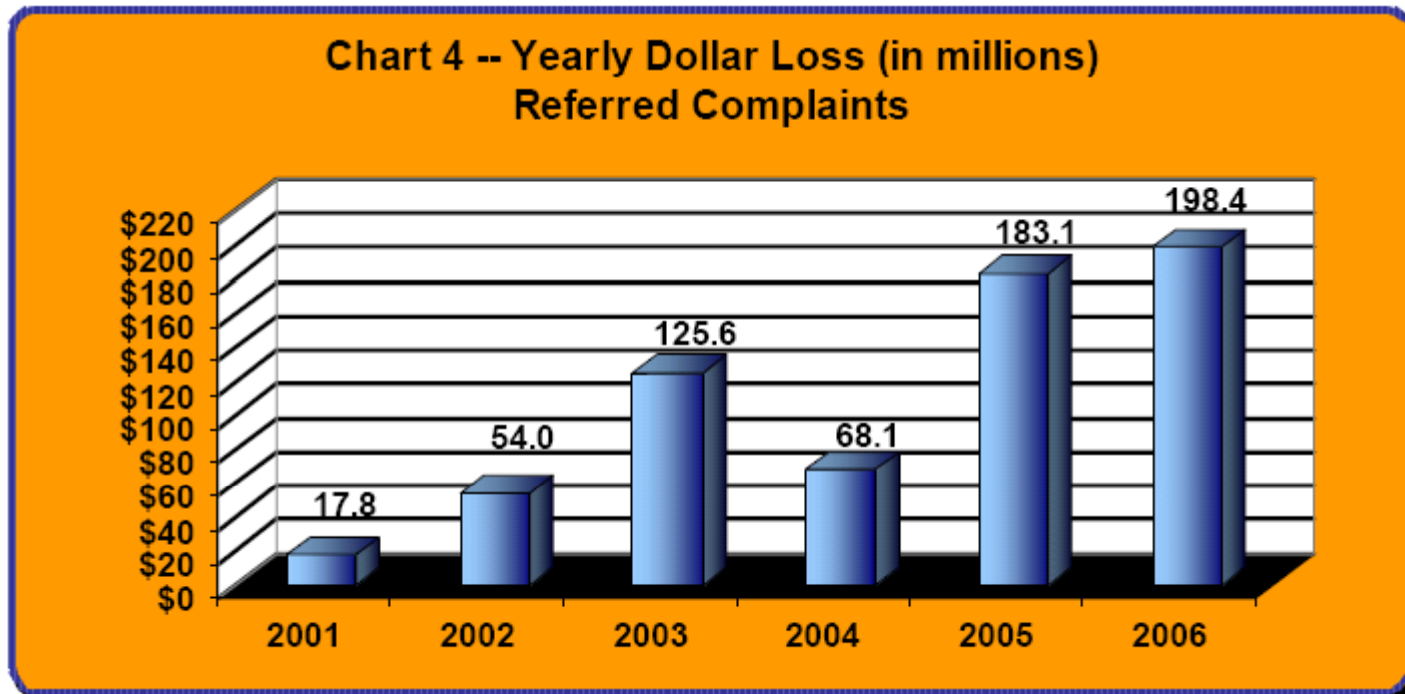
More than a quarter of a million ID theft complaints were lodged with the agency last year, accounting for 36% of the 674,000 complaints the FTC received. That number is down slightly from 2005, when ID theft accounted for 37% of all complaints.

This marks the seventh consecutive year that identity theft has been ranked No. 1. The second-largest number of complaints, 7%, came from consumers who were unhappy with products they had ordered from catalogs.

Internet-related complaints were up, too. According to the 2006 data, they made up 60% of all fraud complaints. Last year, they accounted for 46%.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010764&intsrc=article_more_bot

FBI Cyber-Crime Report for Calendar 2006

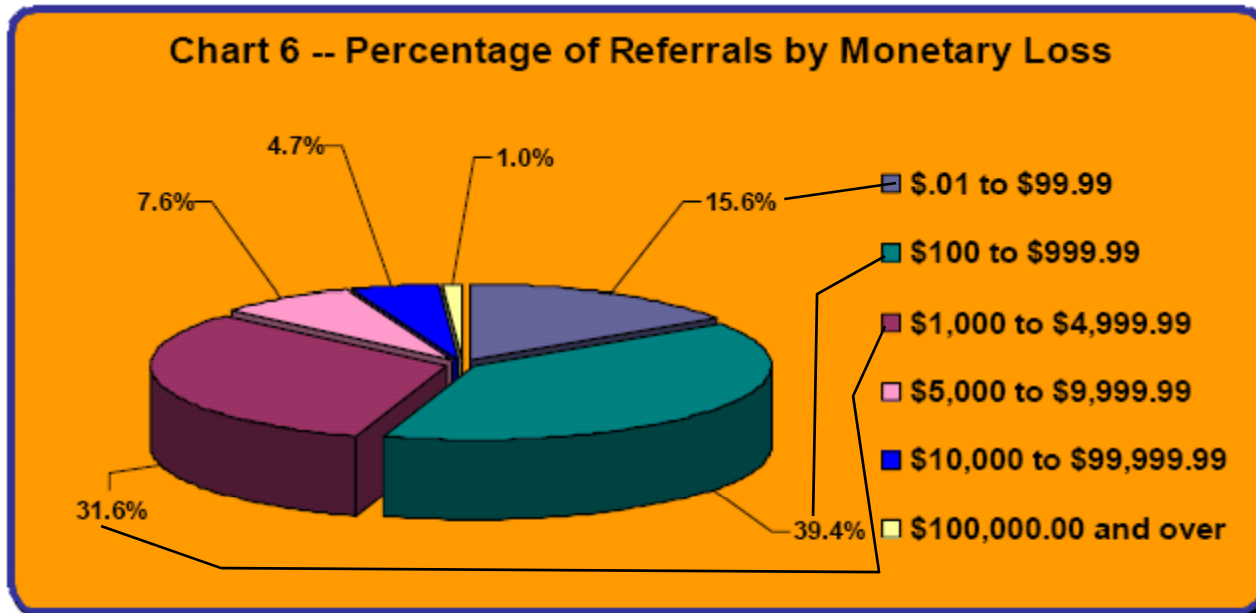


The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants, however the data represents a sub-sample comprised of those complaints that have been referred to law enforcement. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainant, it is estimated that over 90% of all complaints were related to the Internet or online service.

http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

CSER March 2007, rick.dove@stevens.edu, attributed copies permitted

Complaint Type	% Reported Tot \$ Loss	Median \$ Loss Reported
Nigerian Letter	1.7%	\$5,100
Check Fraud	11.1%	\$3,744
Investm'nt Fraud	4.0%	\$2,695
Confidence	4.5%	\$2,400
Auction Fraud	33.0%	\$602
Non-Delivery	28.1%	\$585
Cred/Deb Card	3.6%	\$428



Former Michigan County Treasurer Allegedly Embezzled State Funds to Pay Nigerian 419 Scammers

SANS NewsBites

January 26, 2007

Former Alcona County (Michigan) Treasurer Thomas Katona has been arraigned on nine felony counts of embezzlement and one felony count of forgery for allegedly embezzling state funds to the tune of US \$1.2 million; some of the money was allegedly sent to 419 fraudsters in Nigeria. Katona also allegedly lost more than US \$72,000 of his own money in the scam.

www.theregister.co.uk/2007/01/25/treasurer_accused/print.html

www.michigan.gov/ag/0,1607,7-164-34739_34811-160250--,00.html

www.informationweek.com/showArticle.ihtml;jsessionid=UKVFNGXFCRYXIQSNDLPCKH0CJUNN2JVN?articleID=197000242

[Editor's Note (Schultz): It is hard to understand how someone who ostensibly is an otherwise intelligent, responsible person could allegedly have fallen for such a scam in such a big way.

(Liston): The common misconception is that 419 scams (and their ilk) are aimed at unintelligent victims. ... Remember: scams are aimed at other human weaknesses -- not "stupidity."

Exploit Packs and Hacking Software

SANS NewsBites

January 26, 2007

More than 70 percent of web-based attacks in December 2006 can be traced to just one "multi-exploit hack pack." The kit comprises as many as a dozen exploits, some of which have their origins in proof-of-concept code released by a researcher during July's "Month of Browser Bugs." In a separate story, a Russian crime group is reportedly selling bank account hacking software in South Africa.

<http://www.informationweek.com/story/showArticle.jhtml?articleID=196902970>

<http://www.thestar.co.za/index.php?fArticleId=3642294>

[Editor's Note (Ranum): Yet we continue to hear people spout the ideology that these "security researchers" are offering the community a valuable service and that disclosing bugs is to everyone's benefit. How much longer can people continue to ignore the obvious?]

Security expert cracks RFID chip in U.K. passport

IDG News Service, March 06, 2007

Consultant's demonstration raises new concerns about the security of data in RFID chips

The attack, which uses a common RFID (radio frequency identification) reader and customized code, siphoned data off an RFID chip from a passport in a sealed envelope, said Adam Laurie, a security consultant who has worked with RFID and Bluetooth technology. The attack would be invisible to victims, he said.

"That's the really scary thing," said Laurie, whose work was detailed in the Sunday edition of the Daily Mail newspaper. "There's no evidence of tampering. They're not going to report something has happened because they don't know."

The attack was executed while the passport was still in its original envelope used to send it from the passport service, since RFID chips can be read from a few inches away, Laurie said. He used a passport ordered by a woman affiliated with No2ID, a group that opposes the U.K.'s biometric passport and ID card programs.

http://www.infoworld.com/article/07/03/06/HNexpertcracksrfidchip_1.html

RFID Chips in Car Keys and Gas Pump Pay Tags Carry Security Risks

Photos by Will Kirk



A popular radio-frequency ID system that is used to deter car thefts and as a convenience device for the purchase of gasoline can be defeated with low-cost technology, computer scientists from The Johns Hopkins University and RSA Laboratories have determined.

The researchers uncovered the vulnerability while studying the Texas Instruments Registration and Identification System, a low-power radio-frequency security system used worldwide. The researchers said that more than 150 million of these transponders are embedded in keys for newer vehicles built by at least three leading manufacturers. The transponders are also inside more than 6 million key chain tags used for wireless gasoline purchases. The computer security researchers discovered a way that tech-savvy thieves can get around the encryption safeguards in these systems.

The research paper has been posted online at: rfid-analysis.org/.

50% of Finance Mgrs Put Unsolicited USB Drive in Computers

SANS NewsBites

January 26, 2007

As a research project, a consulting firm sent USB sticks to finance directors at 500 firms in the UK. The memory devices purported to be invitations to "the Party of a Lifetime" with an anonymous sender but were actually part of an experiment. Nearly half of the finance directors inserted the stick into company computers.

Media companies fared the worst in the experiment, with 65 percent putting the memory stick into computers.

At technology, retail and transportation companies, the figure was between 38 and 39 percent. The devices could be used to plant malware on computer systems.

<http://www.vnunet.com/computing/news/2173365/uk-firms-naive-usb-stick>

[Editor's Note (Liston): While this test seems somewhat contrived, you really can't argue with the results. Human curiosity is an incredibly strong motivator that will, more often than not, overwhelm common sense. If you found a USB key laying in the parking lot outside your workplace, what would YOU do? What would the majority of your co-workers do?

Duracell Employee Pleads Guilty to Stealing Trade Secrets

SANS NewsBites

February 6, 2007

Former Duracell employee Edward Grande has pleaded guilty to one count of stealing trade secrets. According to court documents and records, Grande downloaded research about Duracell AA batteries to his computer; he then sent the information to two rival companies. Both companies reportedly sent the information back to Duracell; neither had solicited the information from Grande. When he is sentenced, Grande could face up to 10 years in prison and a fine of as much as US \$250,000.

http://www.washingtonpost.com/wp-dyn/content/article/2007/02/02/AR2007020200906_pf.html

Buffer Overflow Flaw in Snort

SANS NewsBites

February 2007

A buffer overflow flaw in Snort intrusion detection software could be exploited to run arbitrary code remotely and possibly access data in vulnerable systems.

<http://www.zdnetasia.com/news/security/printfriendly.htm?AT=61991419-39000005c>

<http://www.us-cert.gov/cas/techalerts/TA07-050A.html>

[Editor's Note (Skoudis): This is a pretty serious issue...Disabling the DCE/RPC preprocessor will prevent exploitation of the flaw, but at the cost of making your sensors blind to some very serious attacks. Thus, the "work-around", in my opinion, is a very bad thing in most environments. Bite the bullet and upgrade, please.

(Schmidt): Failure to develop secure applications continues a black eye on the entire development and it is even worse when basic secure code analysis is not used on "security" applications.]

China Steals Data From Military Computers on NIPRNet

SANS NewsBites

August 18, 2006

According to Major General William Lord, director of Information, Services and Integration in the Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer, "**China has downloaded 10 to 20 terabytes of data from NIPRNet.**" Lord says there is no evidence China has managed to penetrate SIPRNet. Air Force Research Labs are investigating possible defensive tactics.

www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn_daily&story.id=41669

(Paller) Major General Lord is simply saying out loud what White House and DoD officials have known for almost three years; that's how long the hacking and data thefts are known to have been going on. **What he did not say was that the same techniques (and attackers) have proven successful in penetrating DoD contractors such as Lockheed Martin and Raytheon, and penetrating many other government agencies including some you would not expect the Chinese military to care about.**

Chinese hackers attack 'anything and everything'

Attacks coming from China, probably with government support, far outstrip other attackers in terms of volume, proficiency and sophistication, said a senior Netwarcom official, who spoke to reporters on background [Feb 12 \[2007\]](#). The conflict has reached the level of a campaign-style, force-on-force engagement, he said.

Chinese hackers gained notoriety in the United States when a series of devastating intrusions, beginning in 2003, was traced to a team of researchers in Guangdong Province. The program, which DOD called Titan Rain, was first reported by Federal Computer Week in August 2005. Following that incident, DOD renamed the program and then classified the new name.

Gen. Ronald Keys, commander of Air Combat Command, told reporters at the conference that [current policies prevent the United States from pursuing cyberthreats based in foreign countries. Technology has outpaced policy in cyberspace](#), he said.

Conflict

To Disclose or Not Disclose

Painful Disclosures. The average stock prices of six companies that had disclosed an information security breach between February 2005 and June 2006 **fell by five percent within a month of the disclosure and remained as much as 8.5 percent below predisclosure levels for nearly a year.**

That damage compounds any harm done to the organization's reputation, not to mention regulatory penalties that have reached as much as \$15 million, according to a research study by Enterprise Management Associates (EMA), an IT management consulting firm.

THE ENEMY IS WITHIN

**Finding and Destroying the Enemies Already Inside Our Networks: A Call For Help
Mason Brown, SANS Institute (January 2007)**

...Evidence is now overwhelming that networks in banks and military organizations, in nuclear labs and military contractors, in civilian agencies and hospitals, in power plants and other critical infrastructure, all have consistently been penetrated, yet we continue to spend almost ALL of our resources on 'more rocks' for thicker walls for perimeter defense.

...We need fresh perspective -- and SANS wants to find the next crop of innovative pioneers who are quietly solving the new problem of dealing with systems and networks that have already been compromised.

...the question is no longer whether we can keep THEM out -- we can't. The question is what we do when they are already in. If we assume the enemy WILL get in -- then we must start to think differently about defense.

Security is Broke

The Facts:

- **Vulnerability** – Increasing points and modes of attack
- **Threat** – Increasing attackers and incidents
- **Risk** – Increasing value available for compromise

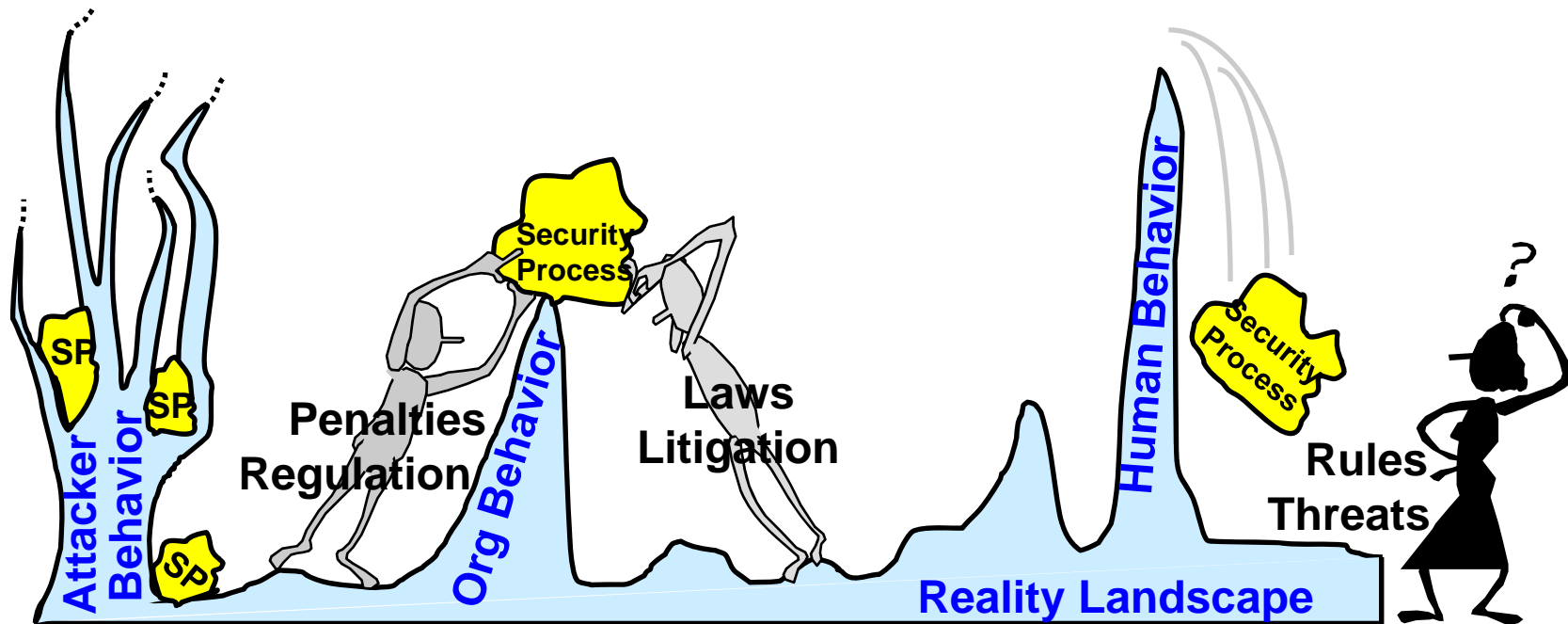
The Results:

- **Time stolen by security measures is increasing**
- **Money invested in security measures is increasing**
- **Effectiveness and life-cycle are decreasing**

Note:

***The stuff you bought and installed last year
doesn't affect this year's attack modes;
but you can't discard it,
you must add new-attack counter-measures continuously***

Maintaining Systems in Unstable States Takes Constant Energy Input



Expecting or enforcing ideal and repetitive behavior ignores reality...
not a substitute for effective strategy

Humans Assessing Risk

493-Person Perception Poll (Sep 2004):

70% more concerned about cyber security than last year...but

30% believe that they are more likely to...

- Win the lottery
- Get struck by lightning
- Get audited by the IRS

40% in the under-25 age group

The Real Odds:

Lottery win.....	00.000000739%
Lightning-stuck..	00.0000102%
IRS audit.....	00.58%
Security-victim...	70%

www.staysafeonline.info/news/NCSACyberSecurityStrawPerceptionPollReport.pdf

Effective Strategy Requires New Understanding

A rational view of the problem:

- Reality bites – what is its nature?
- The problem is bigger than technology – what is its nature?
- The situation is in constant flux – what is its nature?

A rational view of the solution:

- You are compromised – now what?
- Situation in constant flux – what is proactive/resilient security?
- Effective strategy – what is its nature?

Reality Factors

(Seven areas ignored/conflicted with typical security policy)

Human Behavior – Human error, whimsy, expediency, arrogance...

Organizational Behavior – Survival rules rule, nobody's in control...

Technology Pace – Accelerating vulnerability-introductions...

System Complexity – Incomprehensible, unintended consequences...

Globalization – Partners with different ethics, values, infrastructures...

Agile Enterprise – Outsourcing, webservices, transparency...

Agile Attackers – Distributed, collaborative, self organizing, proactive...

**For 50 years of IT-progress...
management policy/procedure/practice
has followed behind ... patching potholes**

Strategy Focus Issues

Strategy - Embodied in Policy, Procedure, and Practice:

Can respond immediately

Can respond anticipatively

Can respond proactively

Can respond effectively

Technology:

Time-lagged reactive backup

Necessary

Can automate learned strategy

Could enable and facilitate proactive and resilient strategies

Systemic Focus Needed on Strategy (Policy, Procedure, Practice)

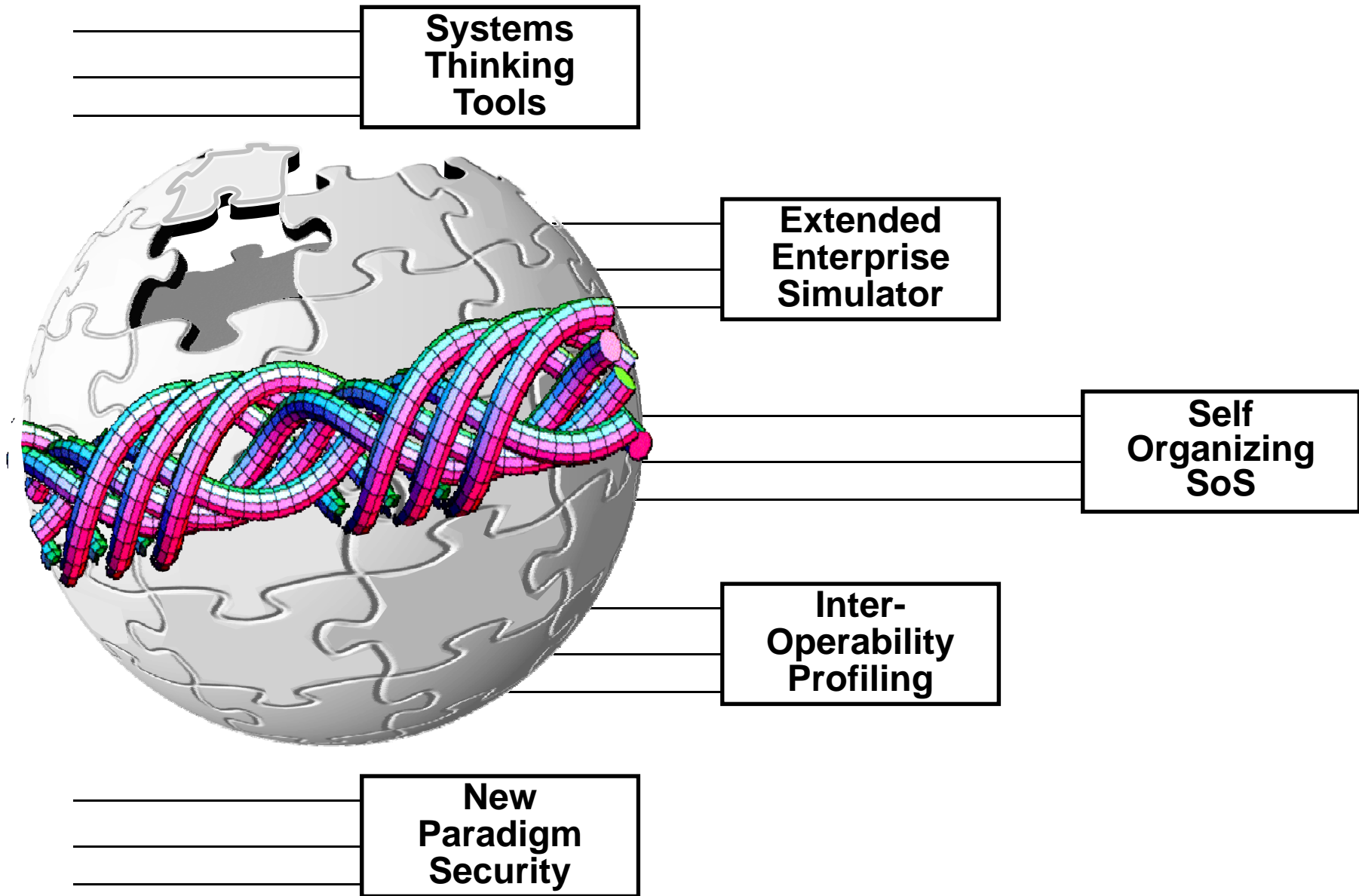
Recognize and accommodate behavior reality

Eliminate cause-effect links

Meet attacker agility with prepared requisite variety (principle)

Mitigate productivity-loss with parsimony/harmony (principles)

Integrated Research Agenda



New Paradigm Security

A Pathfinder-Forum Call-to-Arms

Founded on the premise that security *state-of-practice* is broken, that fixing it will require a paradigm shift in security strategy and practice, and that the initiative must be taken and embraced by those at risk.

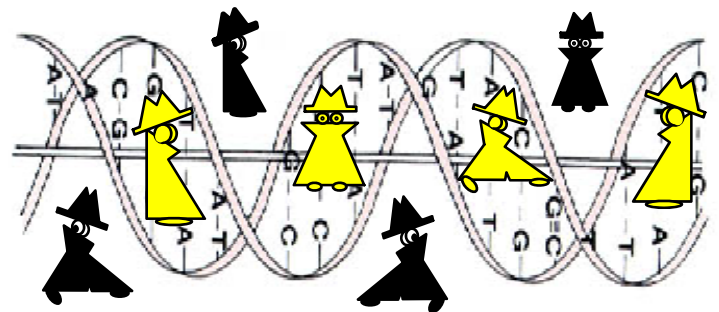
Strategy/policy must:

- Employ holistic systems thinking
- Integrate with enterprise architecture
- Identify and face the realities of the environment:
human behavior, org behavior, tech pace, systems complexity,
globalization, agile enterprise practices, agile attackers
- Assume penetration always and constantly
- Define and address resilient concepts
- Define and address proactive concepts
- Converge physical and cyber security

Technology/practice must:

- Enable and support the above

2007 Critical Infrastructure
Discovery Workshops ...



Pathfinder Forum Concept

Goal – Catalyze distributed community action:

- Create a compelling need to act in the broad community
- Create a core group of knowledgeable, committed, lead-the-way organizations
- Create a roadmap for action

Strategy:

- 20 organizations from a cross section of National Critical Infrastructure
- 3 mos facilitated *discovery* workshops, 3 mos deliverable development
- Participants involved full-time 3-mos, with sponsors on advisory committee
- Aggressive, simultaneous outreach to influential groups in larger community
- Federal co-sponsor (initial matching funds, subsequent S&T initiatives)
- Immediate actionable benefit to participants
- Target summer/fall 2007 start, completed in six months

Deliverables:

- Value Proposition: Compelling stories of new-paradigm security in action
- Roadmap: Technology and knowledge development issues



New Paradigm Security – A Pathfinder Initiative Starting in 2007