Business Aspects of a Secure Adaptive Infrastructure

Evaluating and Mitigating Risk Cost-effectively

Bob Dennis

Mgr, New Business Development
HP/Atalla Security Products Group

Life's (and IT's) great challenge

HP WORLD 2003
Solutions and Technology Conference & Expo

Less filling!

vs.

Tastes great!

Could both be right ?????

Life's (and IT's) great challenge

HP WORLD 2003
Solutions and Technology Conference & Expo

Business has gotten MUCH more complicated!

Finance is the language of the boardroom

HP WORLD 2003
Solutions and Technology Conference & Expo

- 10K
- FASB 146
- TCO
- ROI
- Sarbanes-Oxley
- Accounting of options

Technology is the language of IT

HP WORLD 2003
Solutions and Technology Conference & Expo

- IPv6
- 802.11G
- TCO
- Grid computing
- Kerberos
- IDS
- SSL

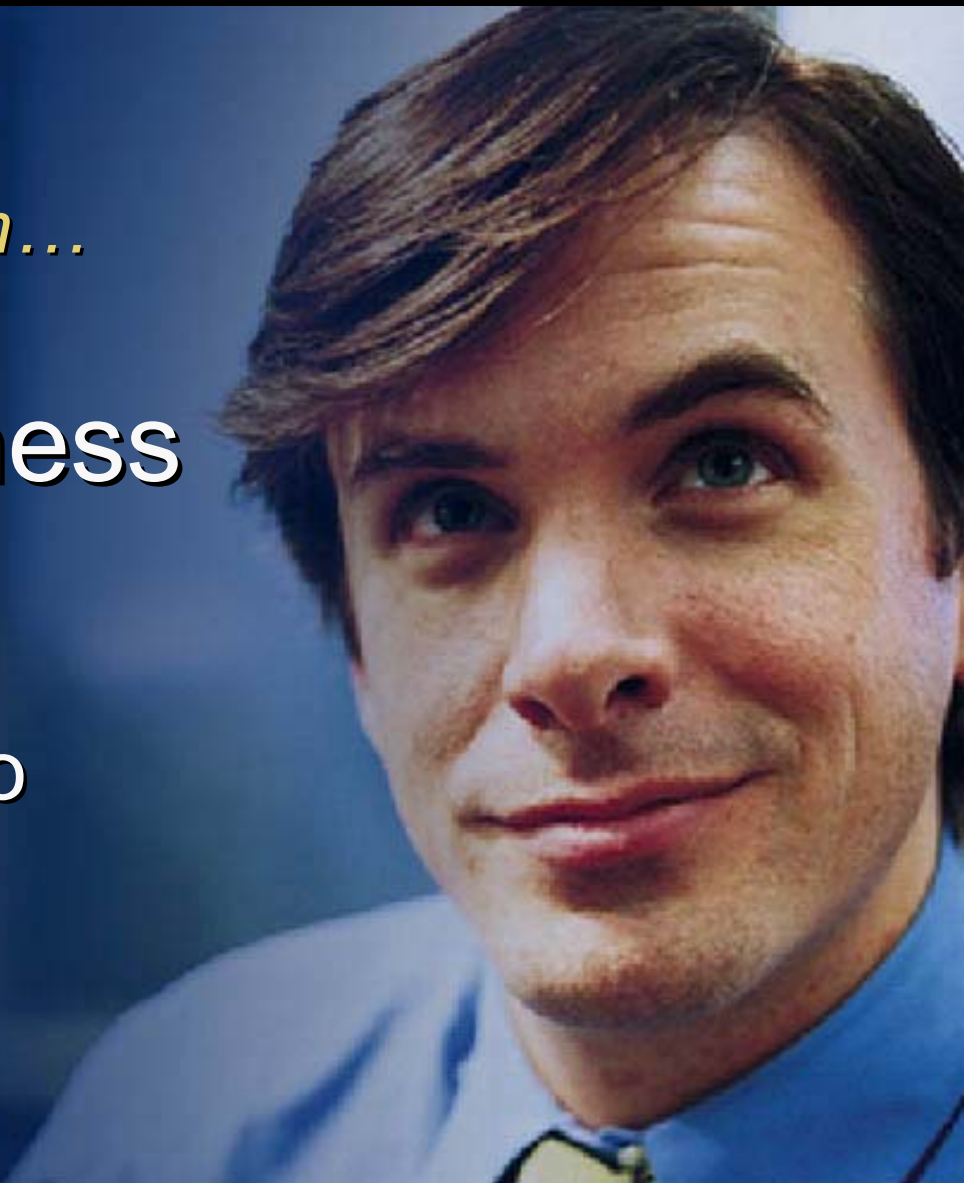
Translation

Message to the boardroom…

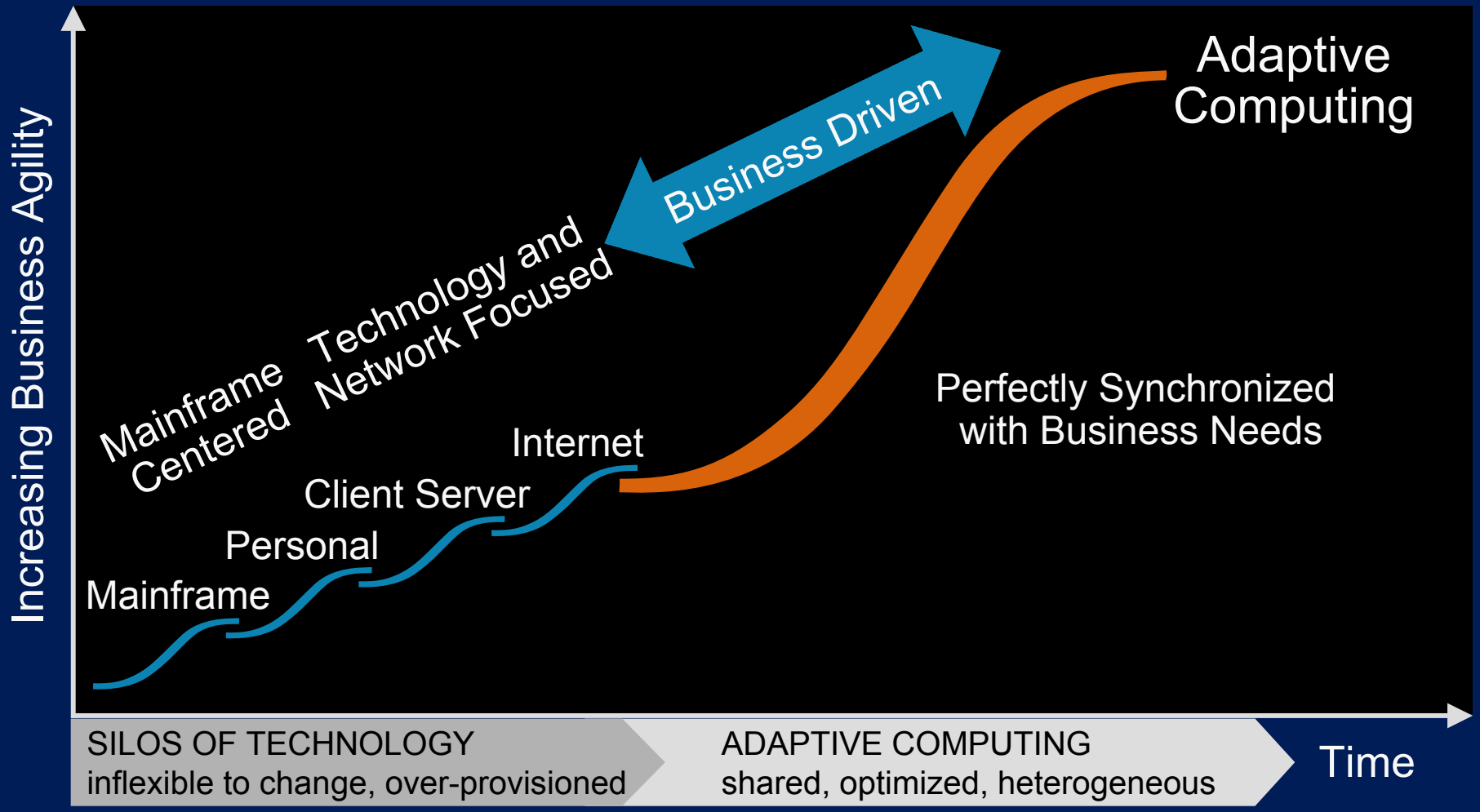
IT is trying to
protect your business

Message to IT…

management is trying to
protect your job



Business needs demand a new model of computing



Today's business challenges require IT to adapt

HP WORLD 2003
Solutions and Technology Conference & Expo

Increased volume of change

Business challenges

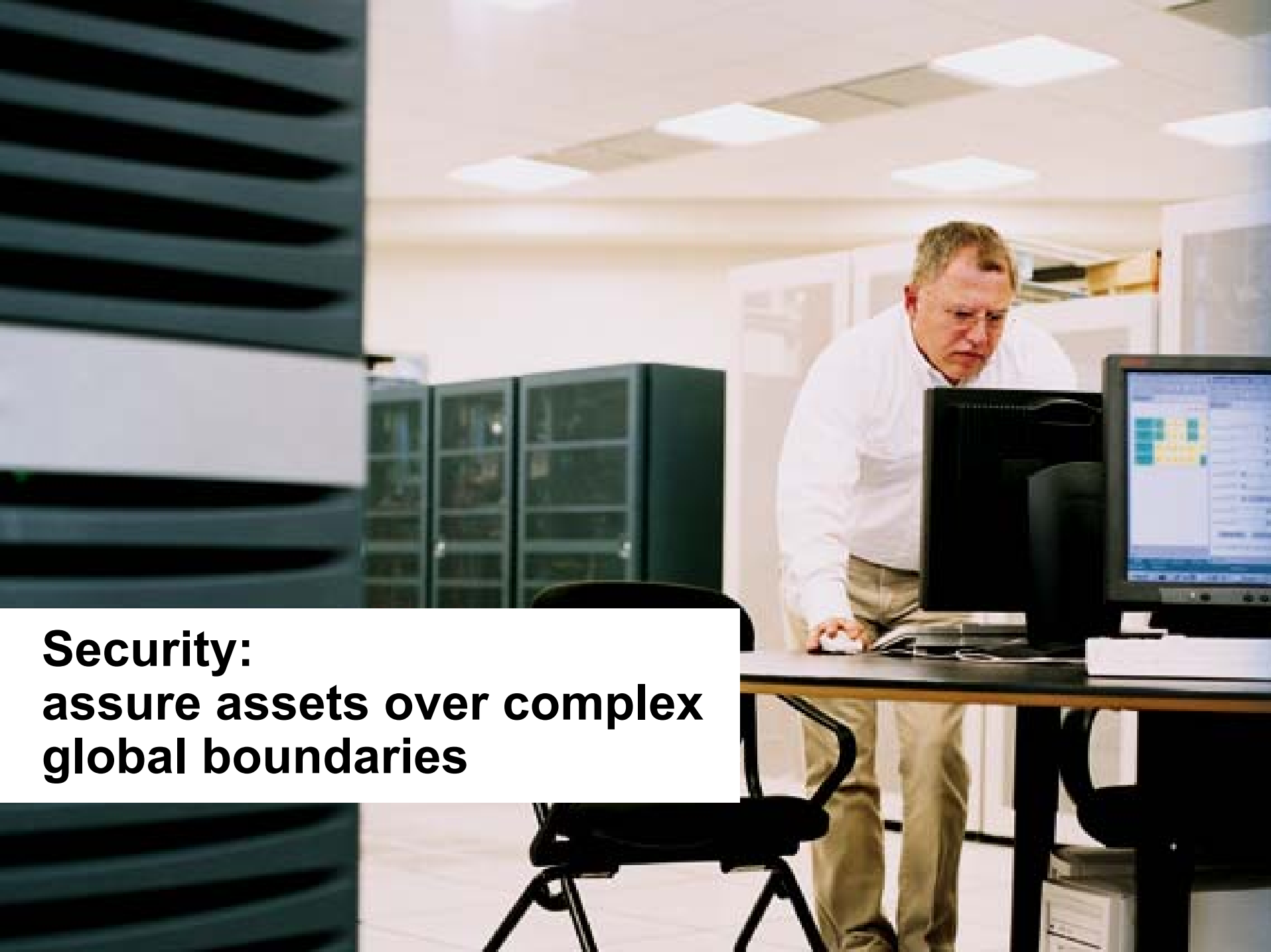
- Improve business performance, quality and ROI, while reducing costs
- **Minimize RISK**
- Associated with change
- Drive new business models and direction
- Shorten time-to-market
- Enable mergers, acquisitions and divestitures

Ability to adapt quickly

IT imperatives

- Link business and IT
- Reduce costs, ensure stability and flexibility
- Reduce complexity
- Optimize assets today and tomorrow
- Extend value and reach of the enterprise

The rush to adapt frequently overlooks secure practices



Security:
assure assets over complex global boundaries

Why trust HP ?

HP systems carry…

- **95%** of all securities exchange transactions worldwide
- **80%** of ATM transactions worldwide
- **66%** of the POS transactions worldwide
- **70%** of the estimated 66 trillion card-based financial transactions worldwide in 2000

HP systems support…

- **75%** of the world's inter-bank electronic funds transfer networks
- **14 of the top 15** stock exchanges (…and over 130 exchanges in total)

The driving forces of infrastructure security

To be effective, security must be applied to…

- User/role management
- Access to resources
- Communications – VPNs, etc.
- Intrusion detection and response
- Public Key Infrastructure (PKI) management
- Software management

Identifying risks — Internal

- Employees
- Employees
- Employees
- Contractors
- Repair personnel

Employees ?

HP WORLD 2003
Solutions and Technology Conference & Expo

ajc.com
The Atlanta Journal-Constitution

PRINT THIS

Click to Print

EMAIL THIS | Close

ajc.com | Business | Hacker may sit in next cubicle[The Atlanta Journal-Constitution: 5/14/03]

Hacker may sit in next cubicle

By BILL HUSTED
The Atlanta Journal-Constitution

The computer hacker wasn't a devious competitor or some brainy teenager sitting at his home PC.

Instead, it was a Coca-Cola employee who slipped into the company's computer system without authorization and downloaded salary information and Social Security numbers of about 450 co-workers.

A recent computer scare at the world's largest soft-drink maker worried it enough to send an

Internal risks

HP WORLD 2003
Solutions and Technology Conference & Expo

CNET tech sites: Price comparisons | Product reviews | Tech news | Downloads | Site map

c|net NEWS.COM TECH NEWS FIRST

Front Page | Enterprise | E-Business | Communications | Media | Personal Technology | Investor

Cracking Windows passwords in seconds

By Robert Lemos
Staff Writer, CNET News.com
July 22, 2003, 7:05 PM PT

If your passwords consist of letters and numbers, beware.

Swiss researchers released a paper on Tuesday outlining a way to speed the cracking of alphanumeric Windows passwords, reducing the time to break such codes to an average of 13.6 seconds, from 1 minute 41 seconds.

THE BIG PICTURE
Read more about passwords

The method involves using large lookup tables to match encoded passwords to the original text entered by a person, thus speeding the calculations required to break the codes. Called a time-memory trade-off, the situation means that an attacker with an abundance of computer memory can reduce the time it takes to break a secret code.

The results highlight a fact about which many security researchers have worried: Microsoft's manner for encoding passwords has certain weaknesses that make such techniques particularly effective, Philippe Oechslin, a senior research assistant and lecturer at the Cryptography and Security Laboratory of the Swiss Federal Institute of Technology in Lausanne (EPFL), wrote in an e-mail to CNET News.com.

Search News.com
Go!
Advanced search

Latest Headlines

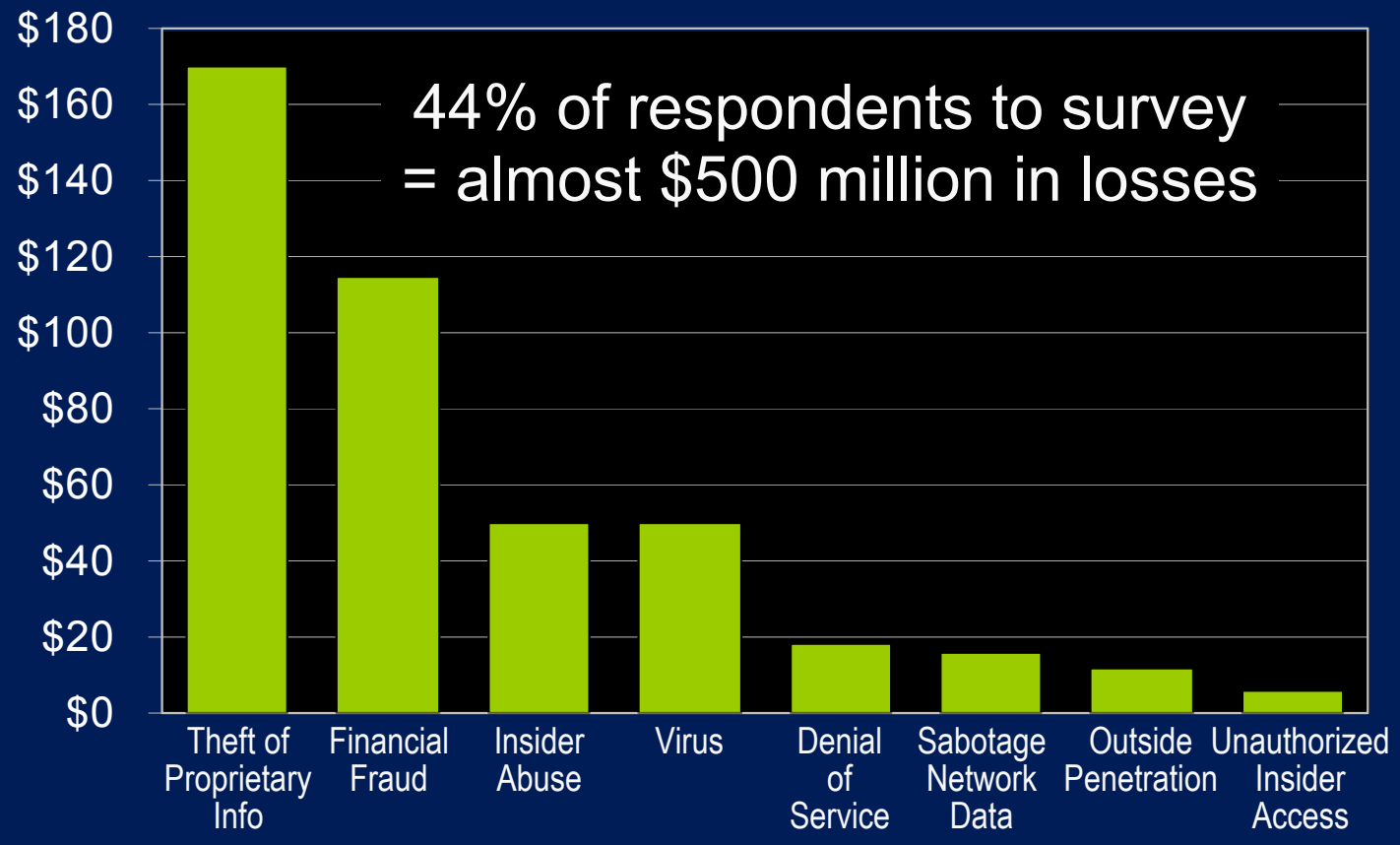
- display on desktop
- AT&T Wireless gears up for 3G launch
- Gateway PDA held back for testing
- Investors search for Ask Jeeves shares
- MarketWatch nabs Pinnacor for $103 Million
- Lawmakers restrict online game in Asia
- Subscriber loss dampens AOL gains
- Lucent posts 13th straight quarterly loss
- HP grabs maker of voice portal software

Identifying risks — External

- Employees
  - Social engineering
  - Loose lips
  - Company data on portable machine stolen
- System penetration by outsiders
- Virus, Trojans, DOS
- Telecom fraud
- Wiretapping (wireline & wireless)

Actual costs

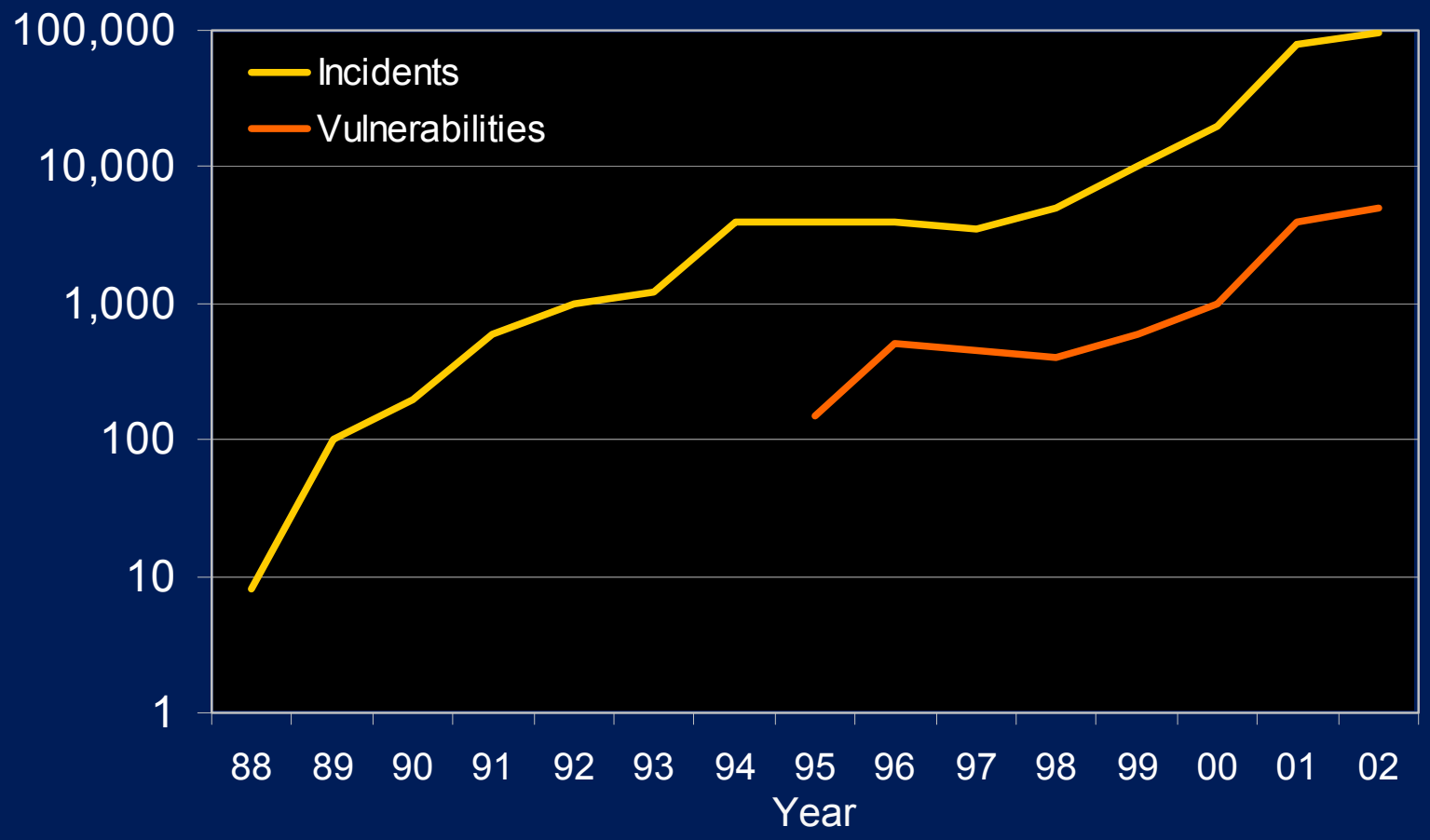
Total annual losses from computer attack ($M)



Source: 2003 CSI/FBI Computer Crime Survey

Risk trends

Computer security incidents and vulnerabilities



Source: Carnegie Mellon CERT Center

Know your downtime cost

Per hour, per day, over 2 days…

Productivity
- Number employees impacted x hours out x burdened hours =

Revenue
- Direct loss
- Compensatory payment
- Lost future revenues
- Billing losses
- Investment losses

Financial performance
- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Damaged reputation
- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Other expenses
- Temporary employees
- Equipment rental
- Overtime and travel costs
- Extra shipping expenses

Placing a value on internal risk

HP WORLD 2003
Solutions and Technology Conference & Expo

Understand the cost

- Downtime
- Intrusion
- Fraud
- Theft
- Loss of customer trust

Placing a value on external risk

HP WORLD 2003
Solutions and Technology Conference & Expo

Loss of proprietary data to competition

Loss of customer trust

- eCommerce
- B2B
- B2C

What's the cost of a security breach?

HP WORLD 2003
Solutions and Technology Conference & Expo

Direct losses

- Lost orders
- Loss of immediate revenues
- Lost productivity

Indirect losses

- Recovery costs
- Damaged competitiveness
- Damage to brand/reputation
- Negative publicity
- Loss of future business
- Impact on stock/political reputation

Legal implications

- Regulatory/legal sanctions
- Legal recourse
- Data Protection Act
- Emerging legislation

Corporate network security

HP WORLD 2003
Solutions and Technology Conference & Expo

*Forrester analyst Ted Julian explains that hacking incidents are **expensive** – not just because of what's taken, but because of the costs associated with cleaning up the mess*

EXPENSE	COST
Returning money stolen from accounts (1,000 accounts @ $1,000 each)	$ 1,000,000
48 hours network downtime beefing up security ($2M/hour)	$ 96,000,000
Emergency audit of 250,000 accounts to look for tampering	$ 1,000,000
PR damage control for three months	$ 6,000,000
Increased fraud premiums	$ 5,000,000
Loss of 10,000 accounts to other banks ($250/account)	$ 2,500,000
Total	**$111,500,000**

Source: Industry standard

Security is critical

Market size and growth ($B)

FORRESTER

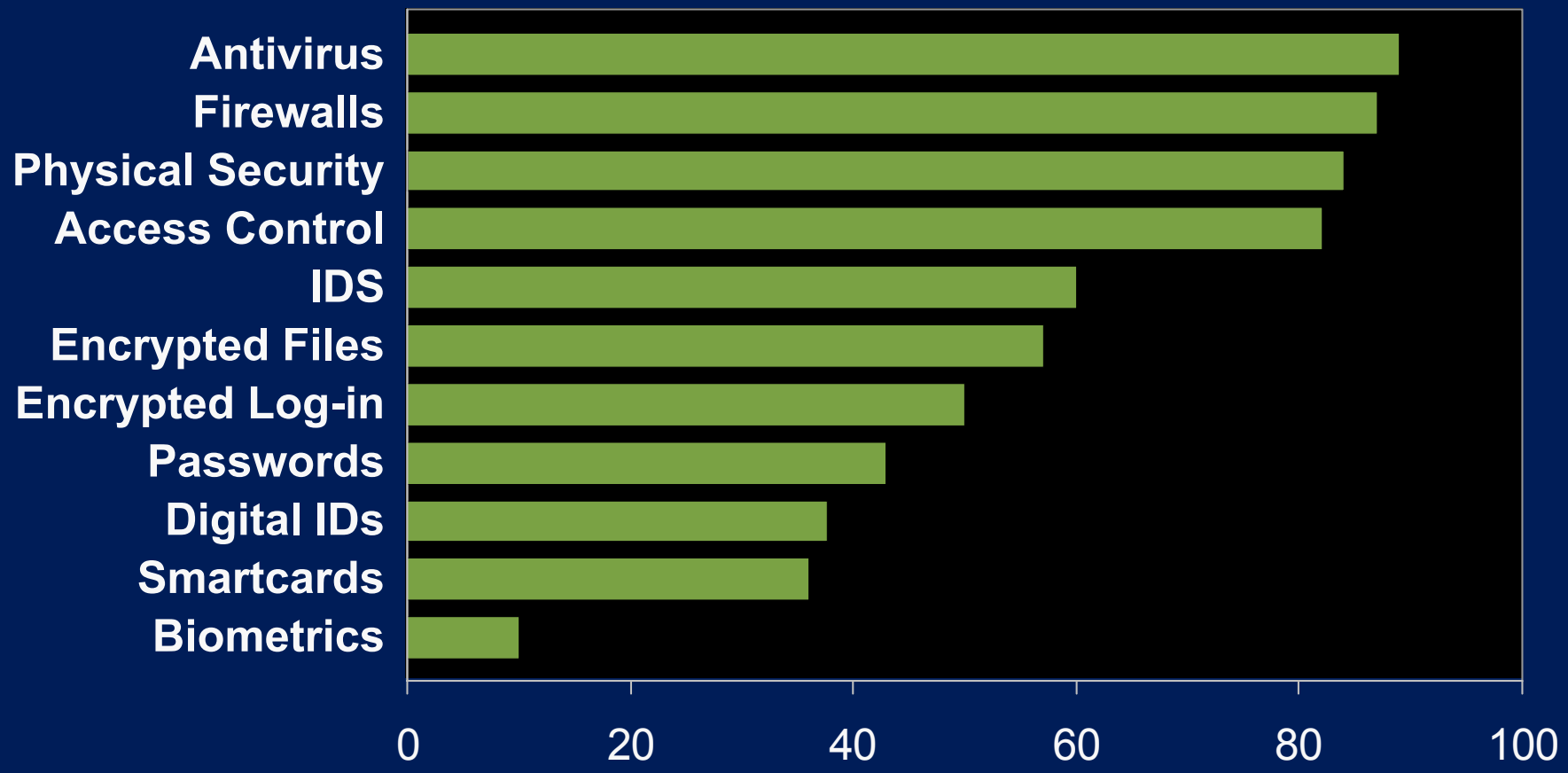
Gartner

"Security and business continuity have the greatest chance of winning approval in enterprises' IT budgets."

Technologies to mitigate those risks

HP WORLD 2003
Solutions and Technology Conference & Expo

Security technologies used



Source: Computer Security Institute

Value of risk-mitigating technologies

Specific cost/benefit analysis

- Adding security card to server
- Why (customer need)?
- Cost
- Benefit(s)

SSL market applications include…

HP WORLD 2003
Solutions and Technology Conference & Expo

Freight shipping records
Digital tickets
Remote access
Real estate assessments
Digital content/property
On-line education
On-line voting
Database access rights
Package tracking
Digital RFP's
Equities trading

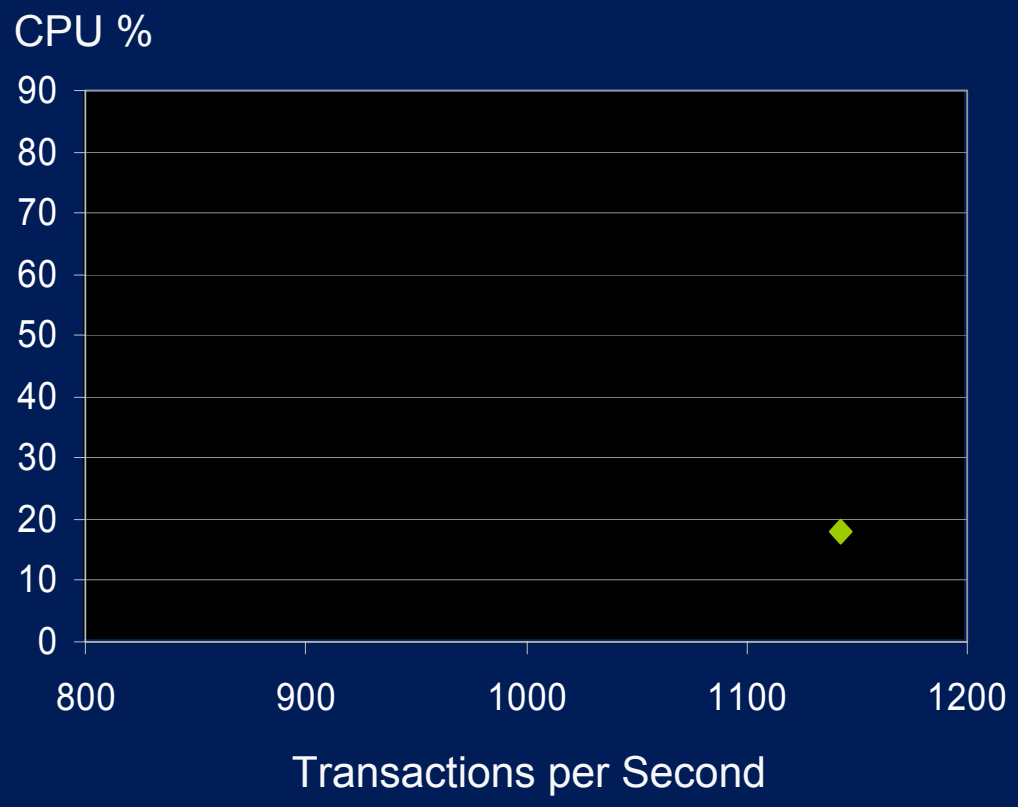
Insurance applications
Access to ISPs
Patient record access
On-line registration
Tax filing
Secure e-mail
Passenger security
Order validation
Account access
Claims processing
Certified software
Prescription rights

Membership rights
Benefits distribution
Professional collaboration
Frequent flyer programs
Access control
Home banking
Physician ID
Software licensing
Legal documents
Voter registration
Payments applications

Example:
Web server without SSL

Compaq DL360, 933 MHz, 2 Pentium III CPUs, 256 MB RAM

- 10k-byte page size
- All http: traffic
- No SSL traffic
- **1143** pages served per second
- **18%** CPU usage
- Lots of 'headroom'



Example:
Web server uses SSL security

Compaq DL360, 933 MHz, 2 Pentium III CPUs, 256 MB RAM

- Change **only 10%** of traffic to SSL
- CPU usage jumps to **80%**
- Total transactions decline to **851** per second
- Where is my headroom now?

Example:
Add HP AXL300 to server

Compaq DL360, 933 MHz, 2 Pentium III CPUs, 256 MB RAM

- No other changes
- CPU Usage drops to **57%**
- Transactions increase to **1081** per second
- 'Headroom' is restored

But what is the business cost (value) ?

HP WORLD 2003
Solutions and Technology Conference & Expo

Environment:

DL380; 2 x 1GHz Xeon

secure web server/eCommerce; Apache 1.3.26; openSSL 0.9.6

Performance:

w/o AXL300	228	1024 bit SSL ops/sec @ 100% CPU
w/ AXL300	466	@ 68% CPU

SSL Efficiency:

w/o AXL300	228 ops/sec / 100% CPU	=	2.28 ops / 1% CPU
w/ AXL300	466 ops/sec / 68% CPU	=	6.85 ops / 1% CPU

*Server productivity improvement = **3x***

But what is the business cost (value) ?

HP WORLD 2003
Solutions and Technology Conference & Expo

Environment:

ML570; 1 x 700MHz Xeon

secure web server/eCommerce; Apache 1.3.26; openSSL 0.9.6

Performance:

w/o AXL300	349	1024 bit SSL ops/sec @ 100% CPU
w/ AXL300	615	@ 45% CPU

SSL Efficiency:

w/o AXL300	349 ops/sec / 100% CPU	=	3.49 ops / 1% CPU
w/ AXL300	615 ops/sec / 45% CPU	=	13.67 ops / 1% CPU

*Server productivity improvement = **4x***

ROI

HP WORLD 2003
Solutions and Technology Conference & Expo

Compare Cost of Additional Servers
to
Cost of SSL Card ($1495)

Increase Life of Existing Servers

Improved Organizational Productivity

ROI

Sometimes ROI is a much simpler issue

- Government regulations
  - HIPAAs
- Customer specifications
  - FIPS 140-2
  - Common criteria
  - B2B requirements

Buyer beware !

Benchmarks can be deceiving

- Different applications have different vulnerabilities and sensitivities
  - SW versions
  - Page size

Speed kills

But what is the business cost (value) ?

HP WORLD 2003
Solutions and Technology Conference & Expo

Environment:

DL760; 8 x 900MHz Xeon

secure web server/eCommerce; Apache 1.3.26; openSSL 0.9.6

Performance:

w/o AXL300	815	1024 bit SSL ops/sec @ 96% CPU
w/ AXL300	536	@ 15% CPU

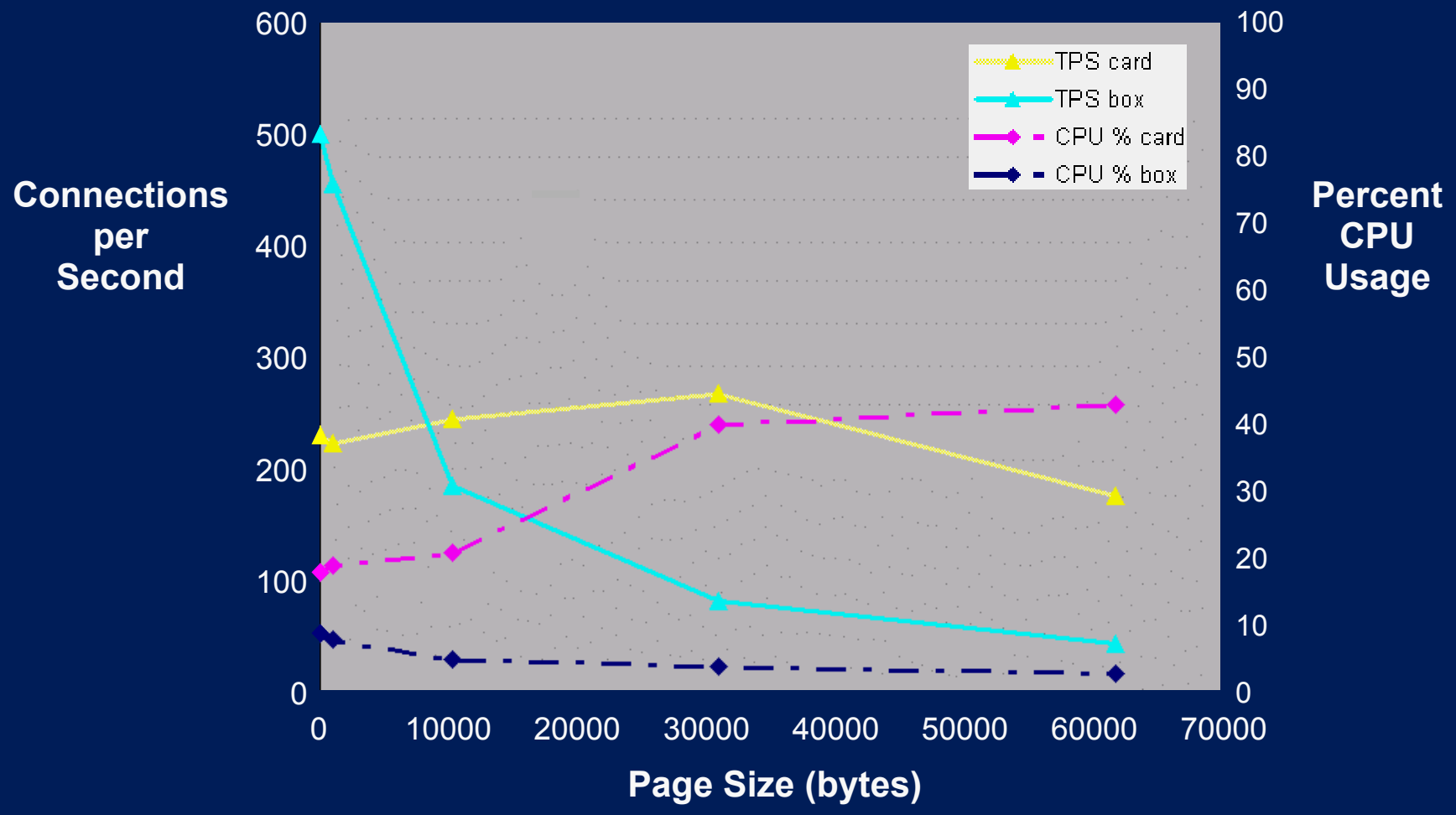
SSL Efficiency:

w/o AXL300	815 ops/sec / 96% CPU	= 8.49 ops / 1% CPU
w/ AXL300	536 ops/sec / 15% CPU	= 35.73 ops / 1% CPU

*Server productivity improvement = **4.2x***

Card vs. appliance

AXL300 PCI card vs. security appliance



Business security solutions from HP

HP WORLD 2003
Solutions and Technology Conference & Expo

Dramatically increasing uptime while ensuring stability

Hardware

- Single system HA servers to OpenVMS to NonStop servers
- Clustering fabric
- Anytime, anywhere storage

Software

- MC/Serviceguard suite
- Multi-OS: HP-UX, Linux® and Windows®
- Range of disaster tolerant offerings
- Security and intelligent monitoring

Services

- Business continuity consulting
- Business recovery services
- Mission-critical support services
- Security services

Partner solution bundles

- CheckPoint
- Nokia
- Oracle® 9i™
- Telecom billing
- ISM

Technology, services and partnerships applied together to create solutions tailored to your unique needs

simplification	modularity
standardization	integration

Business security solutions from HP

HP WORLD 2003
Solutions and Technology Conference & Expo

Ensuring identity, data & process integrity, and continuity

Proven solutions

- Trusted PKI
- Trusted portal
- Security management
- Hardened management
- Policy management

Managed services

- PKI, SSO, Smart Card
- Solution integration services
- Testing and monitoring services
- Policy management

Security services

- Security strategy and governance services
- Planning, design, and implementation services

Platforms

- Authentication, secure OSs, firewall, VPN, encryption, and secure storage
- High availability
- Privacy standards

Technology, services and partnerships applied together to create solutions tailored to your unique needs

simplification	modularity
standardization	integration

Security product solution — hardware

HP WORLD 2003
Solutions and Technology Conference & Expo

Atalla Network Security Processor products

- Business needs
  - Secure customer PINs for ATMs, POS and other devices
- Solution
  - Provides encryption for 85% of ATM transactions worldwide
  - Atalla Key Block (AKB) only method to meet new AXC X9 standards for key management
  - New Secure Configuration Assistant (SCA) offers ease-of-use

HP Atalla Security products organization

- Pioneer in hardware cryptography
- More than 30 years experience
- Depended on by financial institutions worldwide
- Establishes trust imperative for customers to use ATMs
- Based on industry-standard hardware components

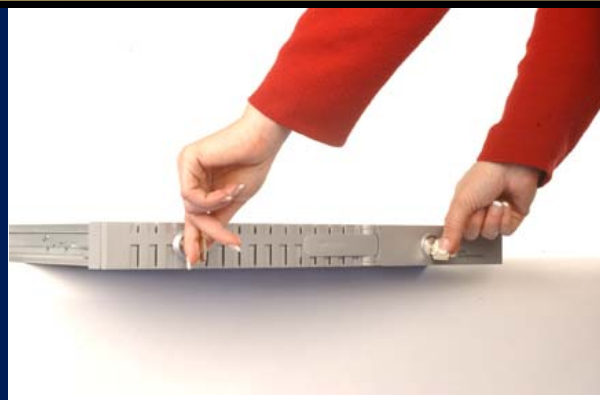
Security product solution — hardware

HP Atalla Ax100 Network Security Processor (NSP) series

- FIPS 140-2 level three certified engine
- Hardened ProLiant 1U platform
- Flexible communications
- Banking personality
- Internet personality
- Secure printing solution

Secure Communication Assistant (SCA)

- Custom SmartCards going for FIPS rating
  - Holds all sensitive data
- Hardened iPAQ device
  - Provides graphical user interface



Security product solution — software

Operating systems

- HP-UX
- Windows SE offerings

Other security software

- Privacy
- Authentication
- Identification
- Non-repudiation

Security services solution

Large European insurer and HP

- Business needs
  - Global security plan
- Solution
  - HP Services to design and implement security standards and processes
- Adaptability and agility achieved
  - Manage global security and governance in times of change
  - Lay foundation for evolving corporate-wide security architecture
  - Protect information assets and reputation as a risk manager

Security services solution

- Healthcare
- Financial
- Email
- B 2 B
- CRM

Security partner solution

HP/CheckPoint firewall solutions

- ProLiant DL Servers
- CheckPoint VPN-1/Firewall-1 software
- Rainfinity's RainWall-S HA software and license
- Security hardened Linux

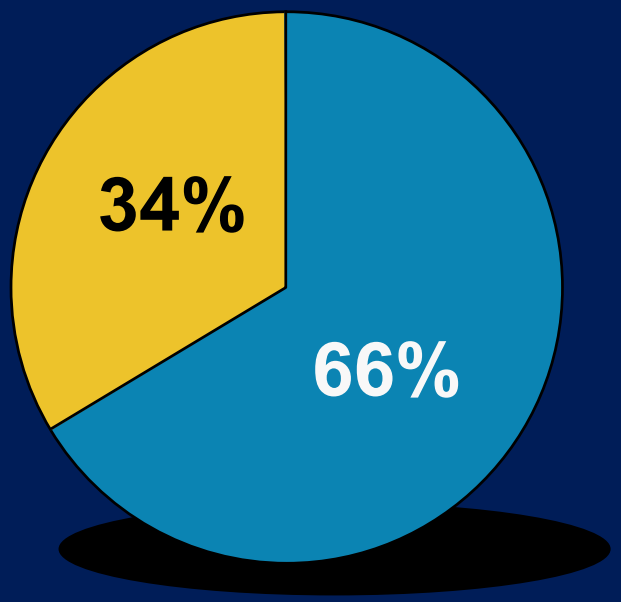
Future security threats

- Faster processors
- More sophisticated cracking tools
- More knowledgeable intruders
- Grid Computing
- Continuing and new OS deficiencies
  - Portables
- RIAA

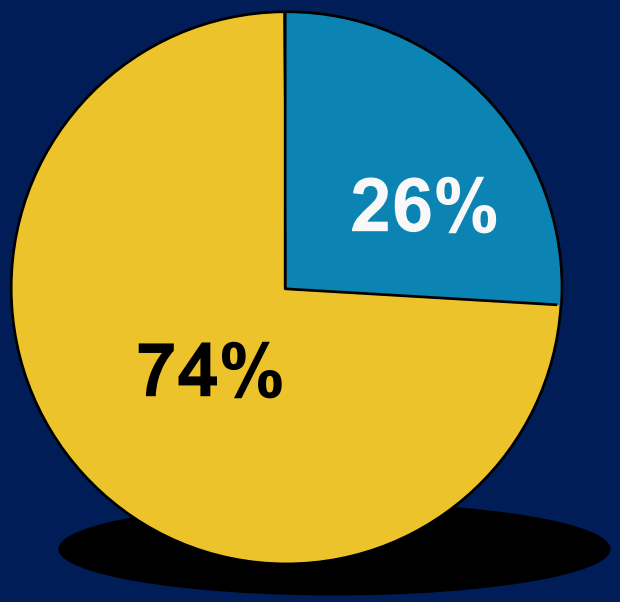
Windows makes an easy target

HP WORLD 2003
Solutions and Technology Conference & Expo

OS of Defaced Web Servers



OS of Internet Web Servers



Windows
UNIX

Future risks — 2

HP WORLD 2003
Solutions and Technology Conference & Expo

ZDNet Where Technology Means Business

SIGN UP ZDNet e-mail newsletters

HOME | NEWS | TECH UPDATE | WHITE PAPERS | DOWNLOADS | REVIEWS & PRICES

Page One | Hardware | Software | Security | Commentary | Headline Archives | Briefs

News Security

PlayStation 3 takes to the grid
By David Becker
CNET News.com
March 21, 2002, 5:00 PM PT

TALK BACK! Add your opinion

Forward in E-MAIL Format for PRINTER

SAN JOSE, Calif.—If distributed computing can unravel the building blocks of life, it can probably help make a better version of "Crash Bandicoot."

That appears to be Sony's thinking as the electronics giant moves ahead with development of the next version of its PlayStation video game console.

Speaking at the Game Developers Conference (GDC), an annual trade show for the creative and technological sides of the game industry, Shin'ichi Okamoto, chief technical officer for Sony Computer Entertainment, said research efforts for the PlayStation 3 are focusing on distributed computing, a

Commentary

BERLIND
David Nagel
Unplugged: Can Palm re-connect?

KOTADIA
Microsoft's patches: Can you trust them?

GOODWINS
Let's see your RFID

MORE COMMENTARY

Latest headlines

PS/3 update

HP WORLD 2003
Solutions and Technology Conference & Expo

Popular Science – Aug 2003 – What'sNew ***Gaming***

"The best rumor heard at (the Electronic Entertainment Expo in LA in July) regarded Sony's patent application for a 'computing architecture and programming model' that many suspect will be the foundation of the next PlayStation. The patent describes several processing centers that break data and applications into uniformly formatted 'software grids' for ultrafast processing, prompting some to claim that PS3 will be 1,000 times more powerful than PS2."

Last word

HP WORLD 2003
Solutions and Technology Conference & Expo

LASEC

[Search] [Home]

- Home
- People
- Research
- Education
- Students Information
- publications
- LASEC for Dummies
- Useful Links
- How to find us

- I&C Home Page
- EPFL Home Page

Advanced Instant NT Password Cracker

Welcome to the web interface of the "Advanced Instant NT Password Cracker" developped by **Luca Wullschleger** and **Claude Hochreutiner**.
based on the faster time-memory trade-off technique developped by Philippe Oechslin at the Laboratoire de cryptographie, EPFL

Submit a request

FAQ

View the result of one request

More informations:

Contact us by mail ntcrack@epfl.ch or read the press:

- Zataz (french).
- Cnet news (english).
- PCtip (german).
- Heise (german).

Last Last Word

BANK FOR INTERNATIONAL SETTLEMENTS

BIS Home > Publications > Committee Publications > BCBS Publications > **Risk management principles...**

Search BIS

Go

Advanced Search

- About BIS
- Press and Speeches
- Links to Central Banks
- Banking Services
- Forum for Central Banks
- Basel Committee
- Financial Stability Institute
- Publications and Statistics
  - Regular Publications
  - BIS Papers
  - Committee Publications
  - Working Papers

Risk management principles for electronic banking

Basel Committee Publications No. 98
July 2003

Executive Summary

Continuing technological innovation and competition among existing banking organisations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits.

The Basel Committee on Banking Supervision expects such risks to be recognised, addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of

Based on these conclusions, the Committee considers that while existing risk management principles remain applicable to e-banking activities, such principles must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of e-banking activities. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. The Committee also believes that the integration of e-banking applications with legacy systems implies an integrated risk management approach for all banking activities of a banking institution.

Final Last Word

25 July 2003
Updated: 14:41 GMT

The Register

Search The Register
Go!

Spam clients outed, credit card details published

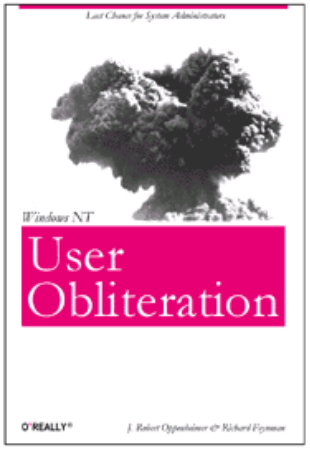
By John Leyden
Posted: 23/07/2003 at 13:36 GMT

Register Services
Register ISP
Reg Jobsearch
Reg Merchandise
IT-minds bookstore

Sections
Front Page
Software
Enterprise Systems
Servers
Storage
Personal Hardware
Semiconductors
Internet
Security
Virus News
Business
Networks
Bootnotes
This Week's Headlines

Anti-spam activists have upped the ante in their fight against junk email by publishing the details - including credit card information - of people who've ordered spamming services online.

CASH'N'CARRION



CASH'N'CARRION

Activists published details from order forms left on a monumentally insecure spam services Web site (http://202.63.201.239), run by notorious American spammer Robert Soloway, on the newsgroup news.admin.net-abuse.email (NANAE). Names, addresses, phone numbers of seven "would-be spammers" were published on the newsgroup last week. Three of those who ordered a $129 spam run or bulk mailing lists from the site come from the UK, three from the US and one from Germany.

Summary

Focus on ROI up front

The earlier the CUSTOMER builds security into IT infrastructures, the higher the ROI

STAGE	ROI
Design	**21%**
Implementation	**15%**
Testing	**12%**

www.cio.com/security

Build security in early to maximize the benefits to your customer

Keep complexity down

- Design security features in from the beginning
  - Higher ROI
  - Reduced complexity (re-work, patches…)
- Keep security as simple as possible
  - Use common encryptions and algorithms
  - Minimize translations and gateways
  - Focus on ease of use – focus on users
- Positive user experience is key to adoption rate
- Look for single vendor accountability

Look for vendors who drive standards

- Standards Development Organizations
  - Int'l, gov't, industry and user
- The Common Criteria and ISO 15408
- BS7799-1 and ISO 17799
- TACD/FIPS/FKMI
- TCPA PC Trust Standard
- PKI Forum
- More

Forrester Research summary

- Companies today under invest in protection
- Corporate threats will intensify
- Smart investments yield big returns

Source: The Forrester Report “Economies of Security”

What's in your wallet !

- Security is an investment; NOT an expense
- Each customer's cost/benefit analysis is different
- How much risk are you willing to assume?

Interex, Encompass and HP bring you a powerful new HP World.