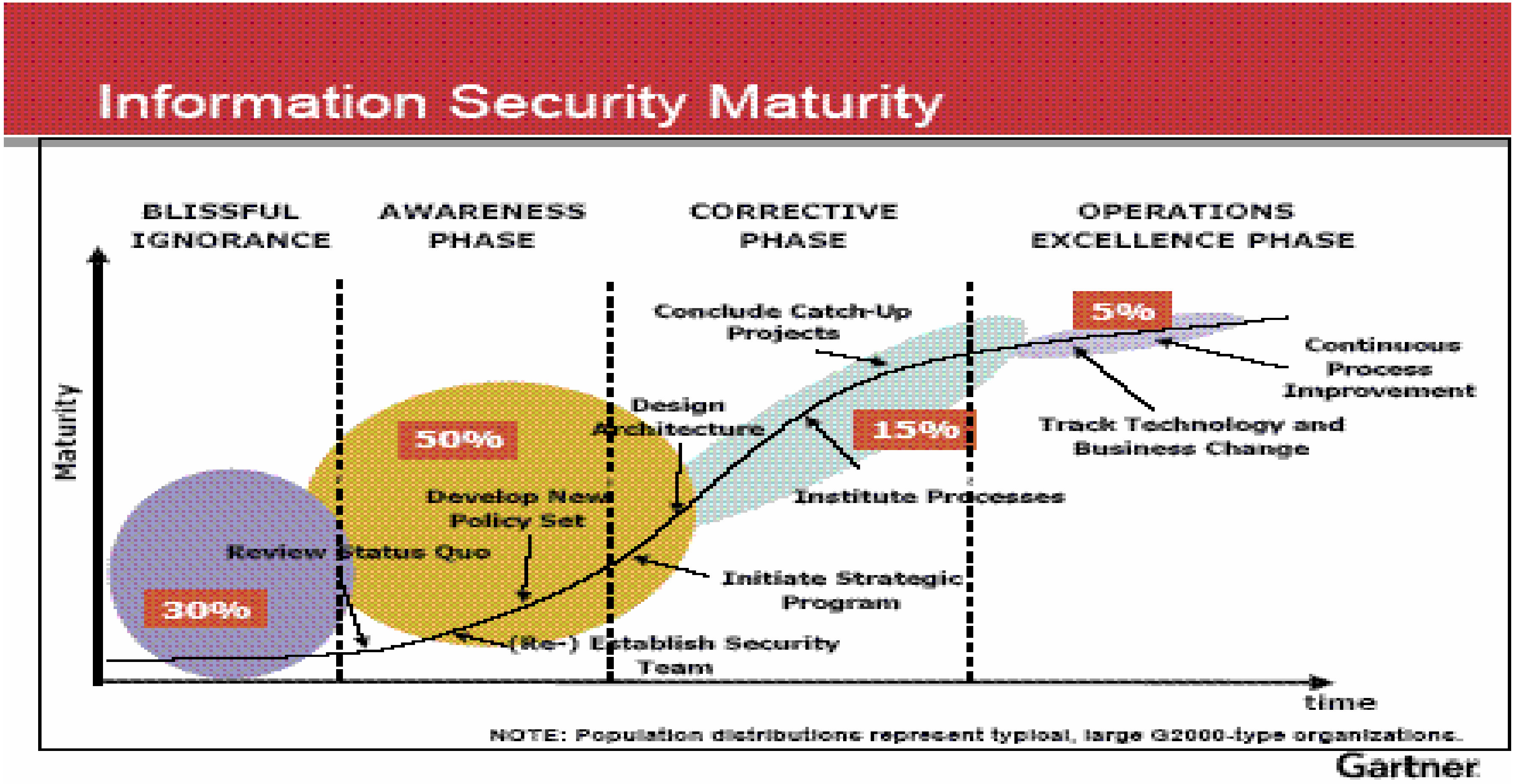
Global Information Security &_IT Security Personnel Development in USA – trend and hurdles

Prof. Howard A. Schmidt
(ISC)2 Security Strategist
Former US White House Cyber Security Advisor

2007/11/14

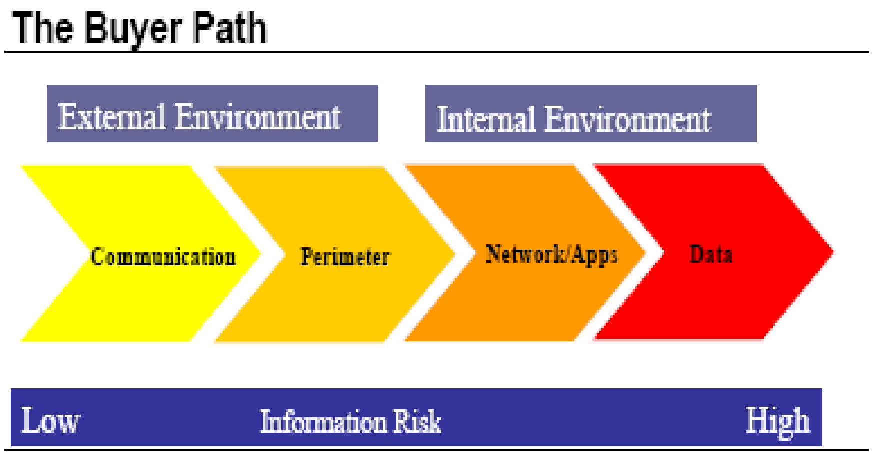
Security & Risk Management

- Security spend as a whole, as a percent of IT budgets, may be leveling off but because (i) targeted, financially motivated attacks continue to rise; (ii) attacks are moving up the application stack; and (iii) new technology waves keep on coming -- there are still <u>numerous emerging threat vectors</u> which require increased spending in certain security sub-segments.

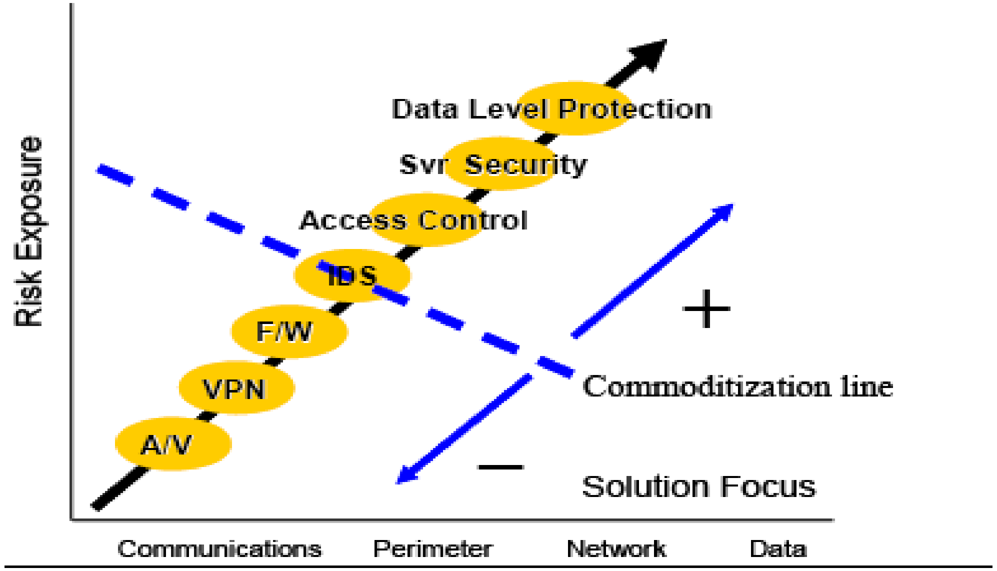


Security & Risk Management

- IT Security is evolving into holistic risk management within organizations
- External, perimeter facing defenses are losing investment to internal, application and data-focused defenses and services based approaches
- Regulatory compliance is as a driver of security initiatives and here to stay
- New products/protocols create new vectors (Wifi, bluetooth, RFID, VoIP, Virtualization, Remote Worker)
- Attacks becoming more organized, targeted and financially driven (phishing, pharming, key logging, man-in-the-middle, identity theft, botnets, data theft)
- Certain sub-segments of security are becoming commoditized, operationalized and embedded into existing O/S, apps, network, chips, etc. (with entrance of large players such as Microsoft, Cisco, IBM, Intel, EMC, Google, HP, Oracle)
- Consolidation of vendors will continue in the security space (convergence and integration of functionality, products, etc.)



Source: Morgan Stanley Research.



Source: Morgan Stanley Research.

Last 12 Months in Review

Major Events

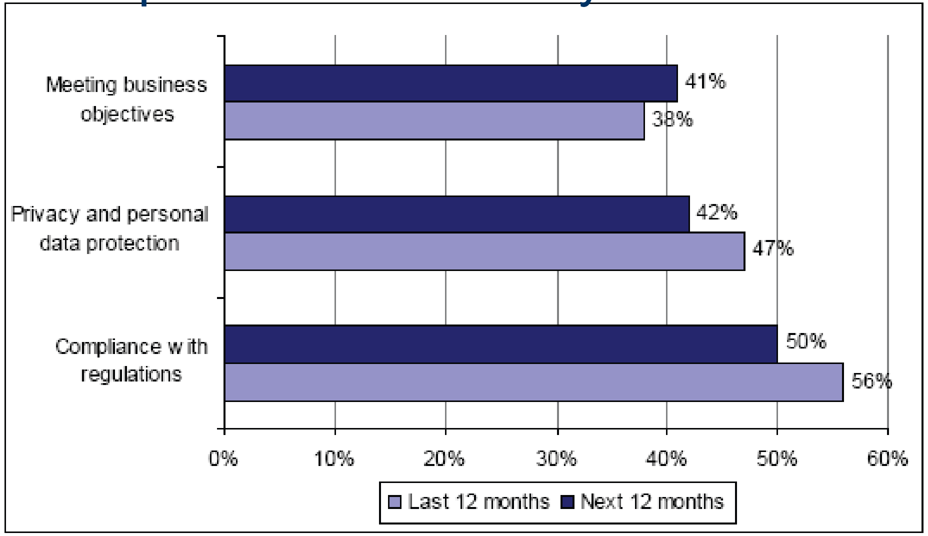
- Infrastructure providers expand into the IT security arena
  - **IBM's $1.1B acquisition of ISS in Aug-06 (Watchfire, Consul)**
  - **Cisco's $830M acquisition of Ironport in Jan-07 (Reactivity)**
  - **Google's $625M acquisition of Postini in Jul-07 (Greenborder)**
- Pure play security vendors augment and enhance differentiation
  - **EMC's $2.1B acquisition of RSA in Jun-06 (Verid, Tablus)**
  - **Check Point's $625M acquisition of Pointsec Mobile Tech's**
  - **Websense – PortAuthority & SurfControl; Secure Computing - CipherTrust; Verisign - Geotrust; McAfee - SafeBoot**
- Windows Vista release
  - **Kernel access; security "enhancements"; inevitable vulnerabilities**
- Identity theft and data loss became even more of a public issue
  - **VA loses personal data of 26M vets / TJX loses 45.6M credit card #'s**
- PCI, FFIEC, GLBA, HIPAA, CA SB1386 continue to evolve at a rapid pace
- Rootkits emerged as a serious threat
- Virtualization and infrastructure consolidation emerge as major trend
- Data retention policies and litigation drive e-Discovery demand

Last 12 Months in Review

Compliance Still Driving Security Spend

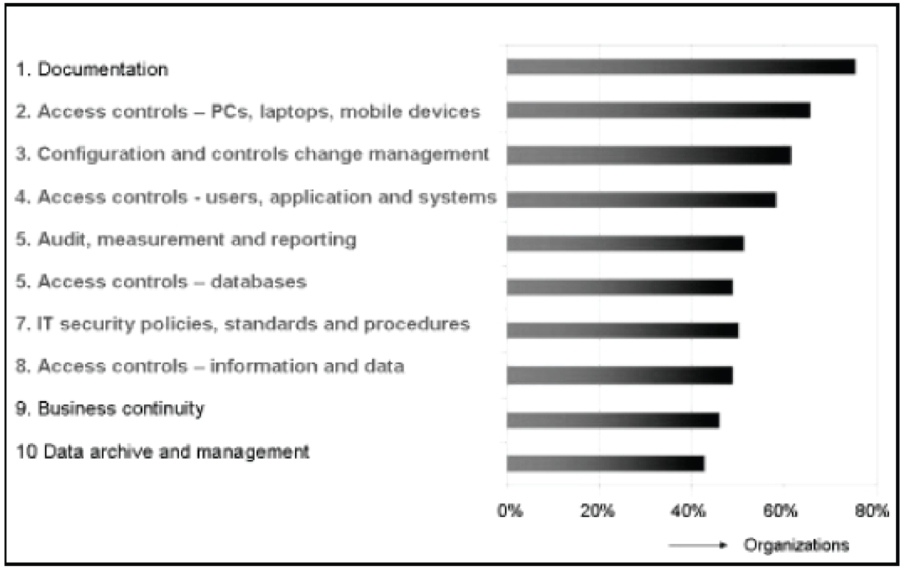
- Compliance is now becoming a key tool for enterprises to evolve a broader view of their infrastructure, processes, and operations.
- According to the IT Policy and Compliance benchmark report in 2006, firms spend about 7-10% of overall IT budgets on compliance-related security spending.
- Regulatory compliance continues to be the top driver of IT security investments in 2007

Top Driver of IT Security Investment



Source: Ernest and Young, 2006 Global Information Security Survey

Causes of Compliance Deficiencies



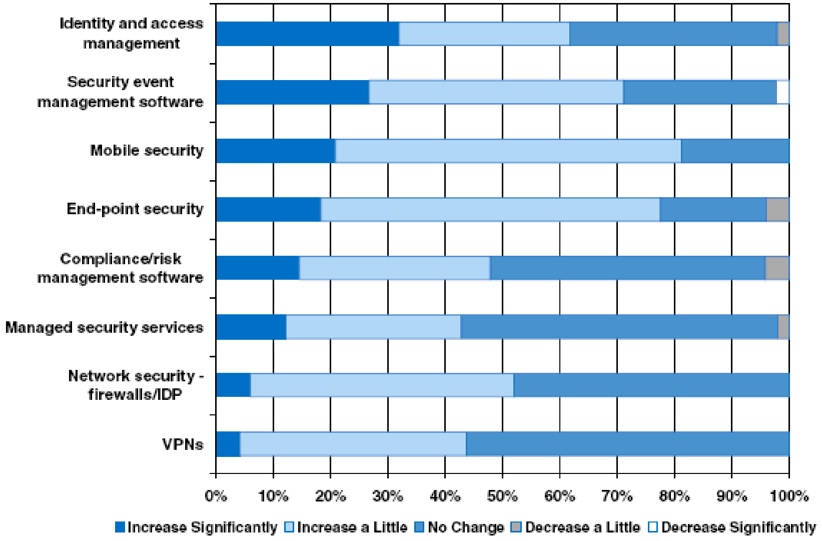
Source: ITPolicyCompliance.com, 2006; Note: Deficiencies from 2-8 are related to IT security

Emerging Threats

Recent Surveys

- IT Security spend remains between 4 – 6% of IT budgets
- Merrill Lynch CISO survey – 62% of CISO's expect increased IT security spending in 2007, 34% flat and 4% decrease

Exhibit 1: Where applicable, please indicate how you expect your spending to change for each product area over the next 12 months, relative to current levels. Please indicate all that apply.



Source: Goldman Sachs Security Spending Survey.

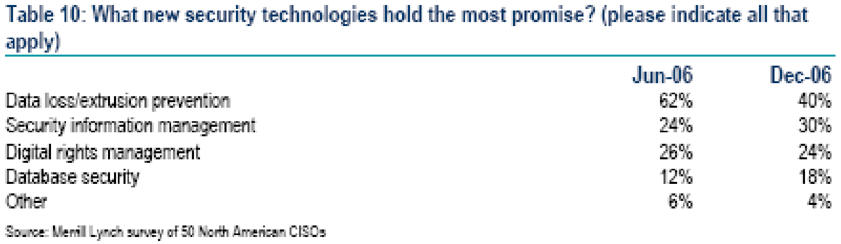


Table 10: What new security technologies hold the most promise? (please indicate all that apply)

	Jun-06	Dec-06
Data loss/extrusion prevention	62%	40%
Security information management	24%	30%
Digital rights management	26%	24%
Database security	12%	18%
Other	6%	4%

Source: Merrill Lynch survey of 50 North American CISOs

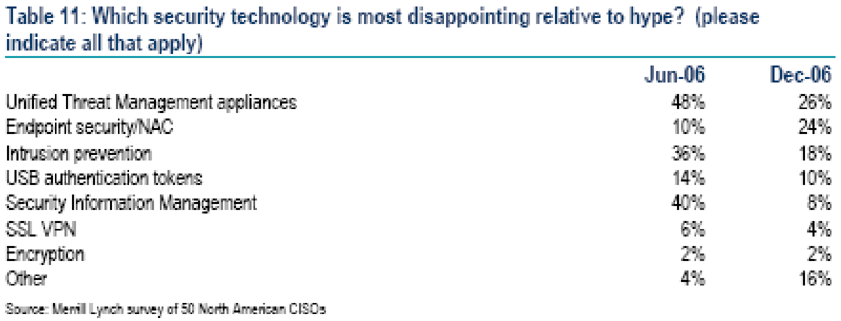


Table 11: Which security technology is most disappointing relative to hype? (please indicate all that apply)

	Jun-06	Dec-06
Unified Threat Management appliances	48%	26%
Endpoint security/NAC	10%	24%
Intrusion prevention	36%	18%
USB authentication tokens	14%	10%
Security Information Management	40%	8%
SSL VPN	6%	4%
Encryption	2%	2%
Other	4%	16%

Source: Merrill Lynch survey of 50 North American CISOs

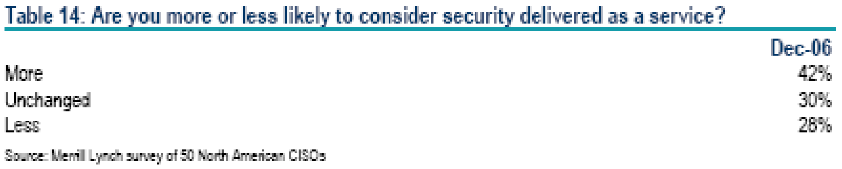


Table 14: Are you more or less likely to consider security delivered as a service?

	Dec-06
More	42%
Unchanged	30%
Less	28%

Source: Merrill Lynch survey of 50 North American CISOs

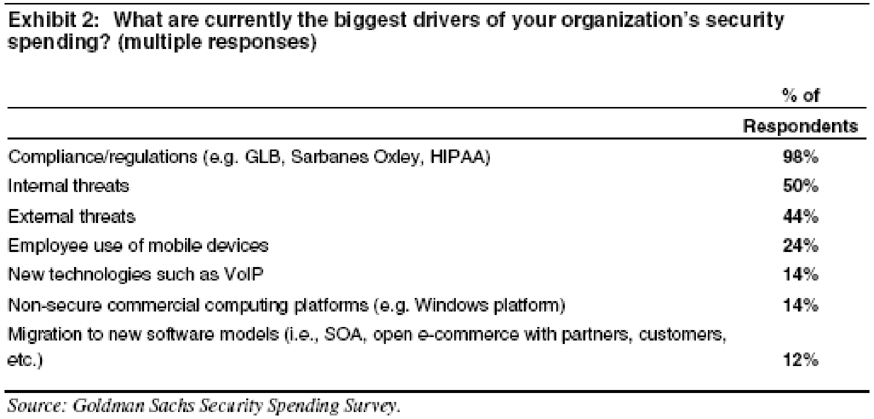


Exhibit 2: What are currently the biggest drivers of your organization's security spending? (multiple responses)

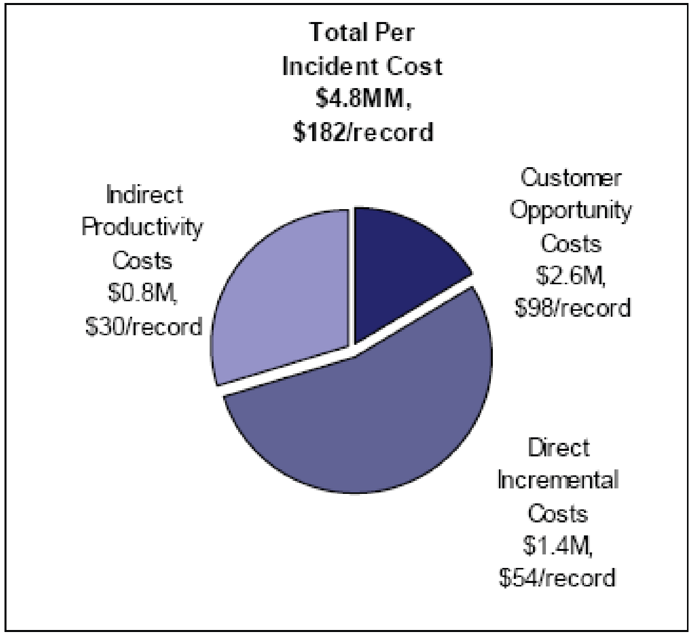
	% of Respondents
Compliance/regulations (e.g. GLB, Sarbanes Oxley, HIPAA)	98%
Internal threats	50%
External threats	44%
Employee use of mobile devices	24%
New technologies such as VoIP	14%
Non-secure commercial computing platforms (e.g. Windows platform)	14%
Migration to new software models (i.e., SOA, open e-commerce with partners, customers, etc.)	12%

Source: Goldman Sachs Security Spending Survey.

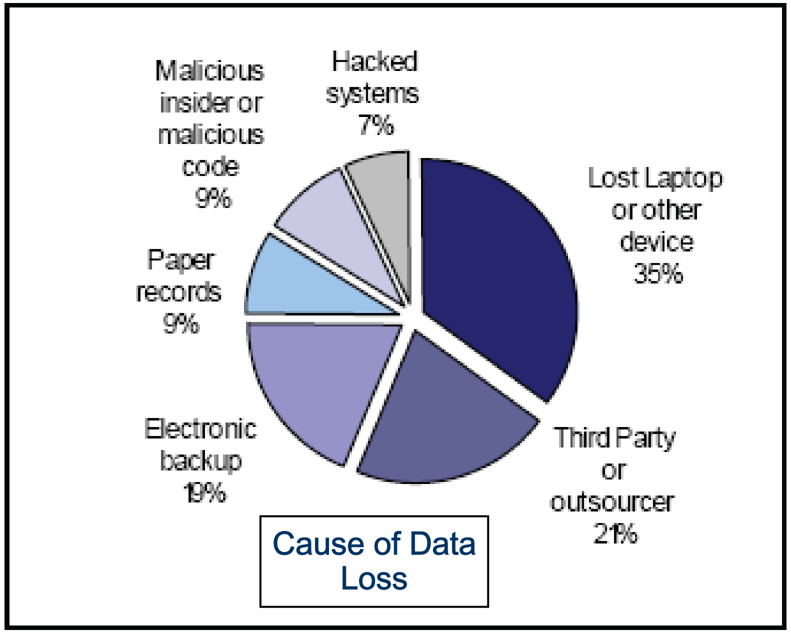
Emerging Threats

Data Breach / Insider Threat

- Insiders represent the biggest threat to confidential data
  - **According to Gartner, insider threats are responsible for about 70% of security breaches. A majority of these breaches are unintentional in nature.**
- According to a study done by the Ponemon Institute, each data breach costs more than $182 per record – an average of $4.8 million per breach.
- According to a study done by the IT Policy Compliance Institute, about 20% of organizations suffer from 22 or more sensitive data losses annually.



Source: 2006 Annual Study: Cost of Data Breach, by Ponemon Institute



Source: 2006 Annual Study: Cost of Data Breach by Ponemon Institute

WiFi is Pervasive

- Mobile Phones

- Laptops

- Home Networks

WiFi is everywhere!

- Other “computing” devices

- Hot Spots

Google WiFi

T · ·Mobile·

BOINGO® WIRELESS

BT Openzone
Wireless broadband
BT

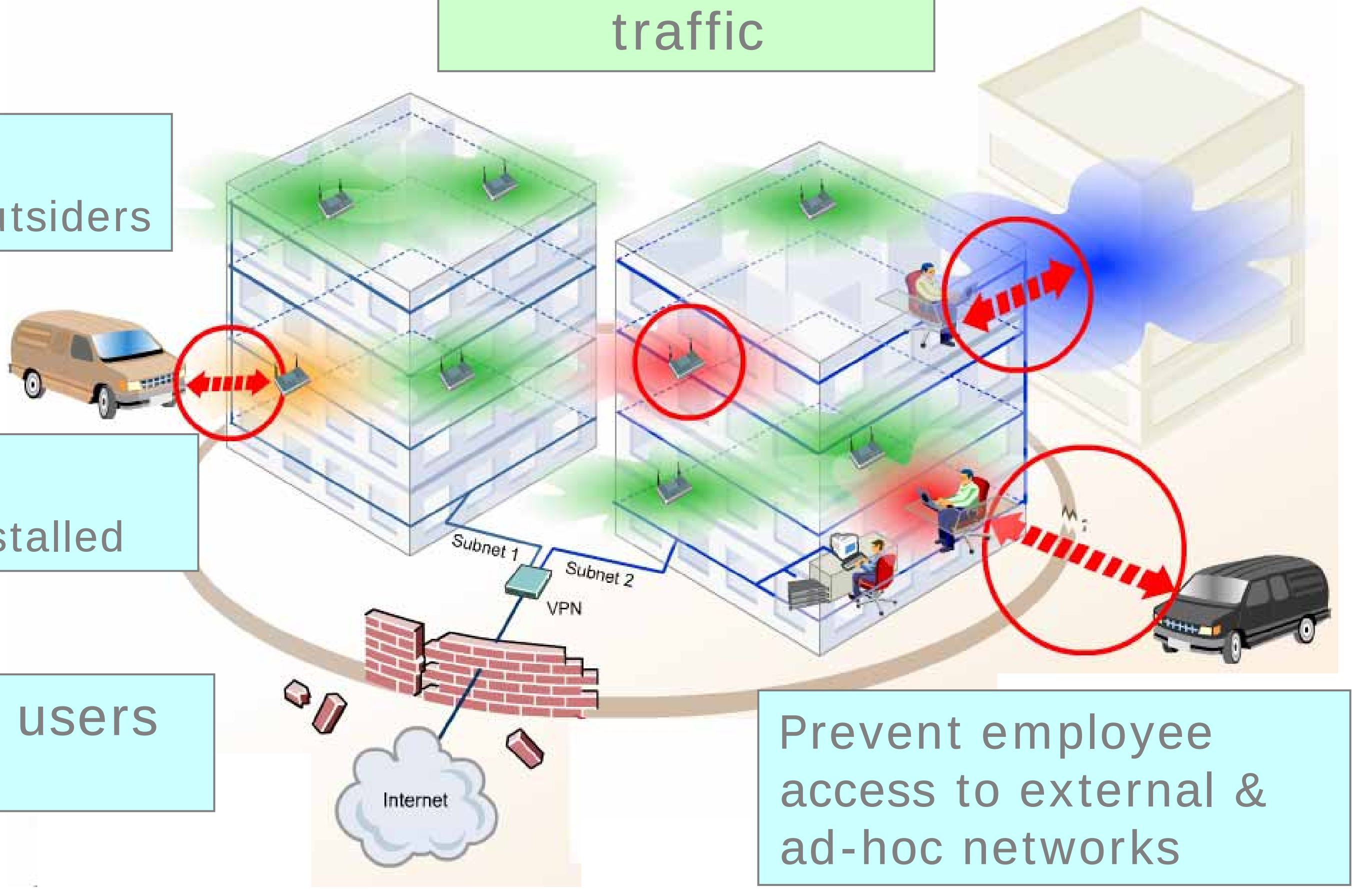
WAYPORT

Wireless Security Policy Elements

Encrypt wireless traffic

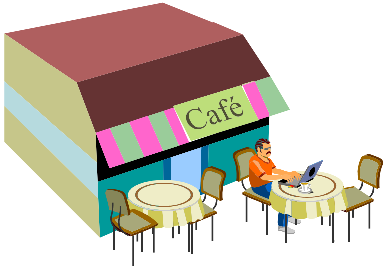
Access control
employees/guests/outsiders

Ban rogue APs
employee/outsider installed



Protect mobile users
on & off campus

Prevent employee access to external & ad-hoc networks



Wireless Policy Can Compromise Wired Policy

Wireless Security Policy Elements

Element	Details	Policy/ Recommendation
Wireless access control	Outsiders include guests/visitors, contractors, vendors/suppliers	No outsider access. Guests/etc – provide password login to isolated VLAN with public Internet access.
Rogue APs	APs installed by someone (employee, consultant, hacker) other than Corporate IT dept	Not allowed.
Accessing external wireless networks	Are employees allowed to use WLANs from neighboring companies/homes, hot spots, muni WiFi, etc.?	Not allowed.
Mobile users/usage	In various locations (home, airports, hotels) – what connections are allowed, what security is required?	At home – require WPA encryption on home APs. Traveling - restrict usage to a limited set of identified wireless ISPs. Require VPN connection in all cases.

You must enforce and monitor these policies whether or not you have deployed wireless.

Diagram of an attack

- **Hacker finds wireless access, e.g.**
  - Open APs
  - Rogue APs
  - WEP encrypted APs
  - Ad-Hoc connections on Laptops
- **Or Hacker creates a wireless trap**
  - Honeypot AP, lures Users to attach

- **Hacker sniffs User IDs and Passwords**

- **Hacker uses User IDs and Passwords to access systems on wired network**
- **Hacker uses system access to install malicious software**
  - Capture payment card (& other) data, communicate data

Wireless Security in Retail

- Wireless = the easiest attack vector for criminals to steal credit card data from retailers
  - **No need to break & enter,**
  - **No physical presence/risk,**
  - **Simply sit in the building across the street and steal to your heart’s content**

Wireless Security in Retail

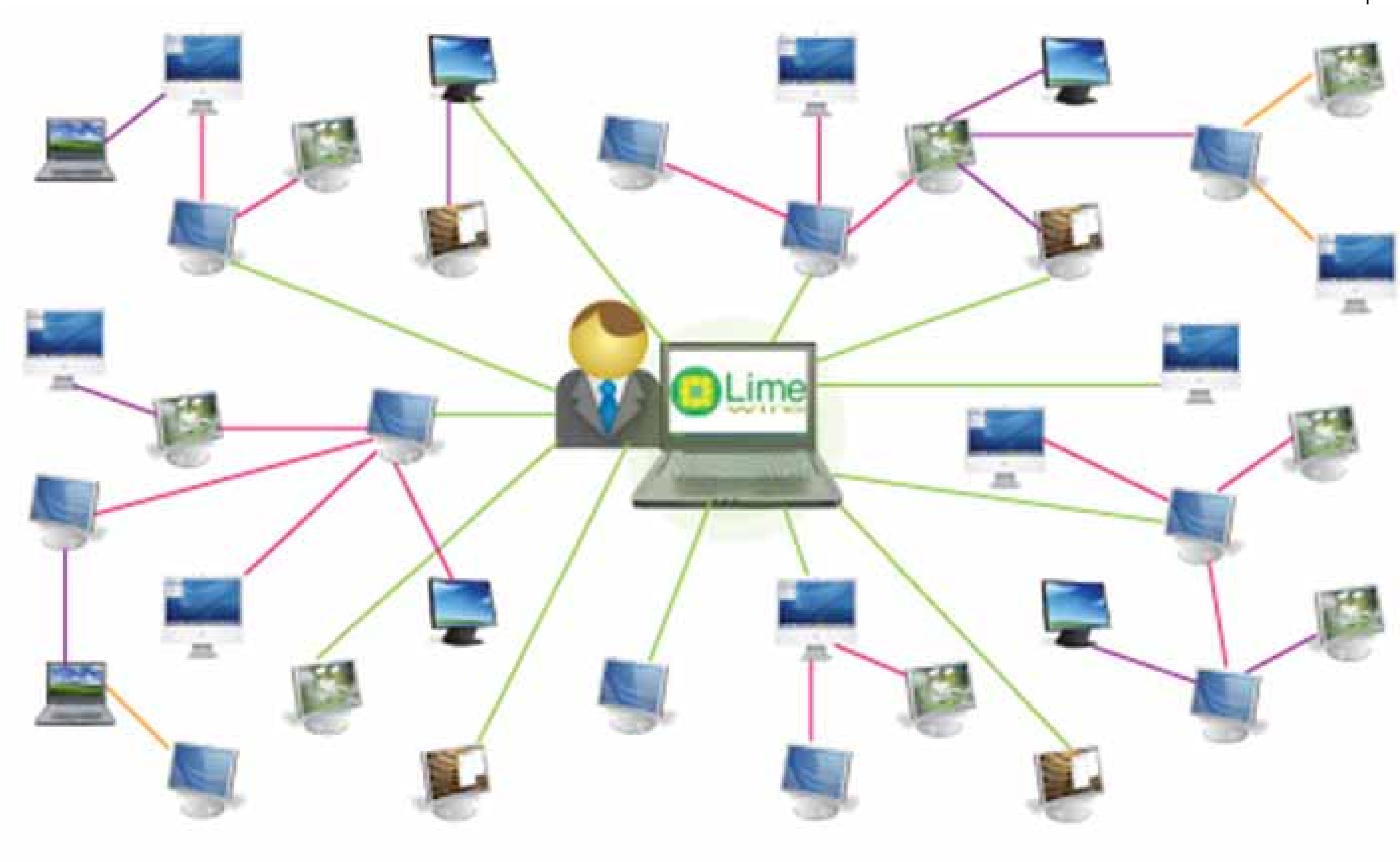
- Wireless creates three groups of attacks/threats:

- Simply reading payment card transactions that are flying through the air (on a wireless link)
  - **Most common threat perception, but smallest risk**

- Using wireless to gain access to the network & attacking the servers – bypassing the firewalls
  - **The TJ Maxx example**

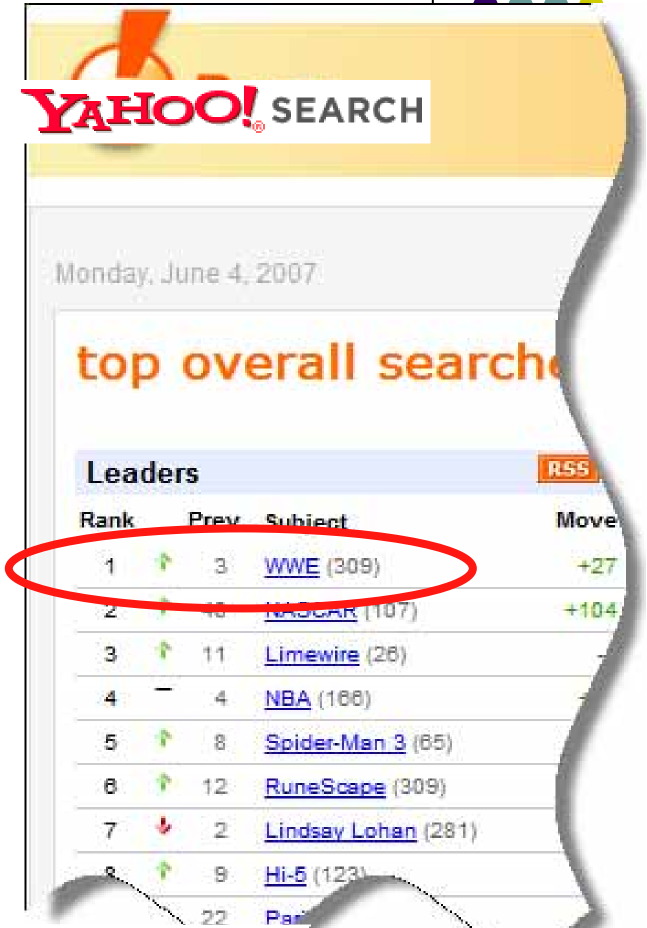
- Insiders (being paid by the bad guys) using wireless to send information out
  - **Take a file of credit account information, log onto the neighbor’s wireless, use Hotmail to send the info to a “friend”**
  - **Not yet publicly documented, but easy to envision**

What is peer-to-peer file sharing?



The WW P2P is large and rapidly growing

- Over 900 million searches a day – larger than Google
- Over 15 billion files on Limewire alone
- Over 450 million copies of filesharing software
- Over 20 million unique users a day
- Over 65% of internet bandwidth



YAHOO! SEARCH

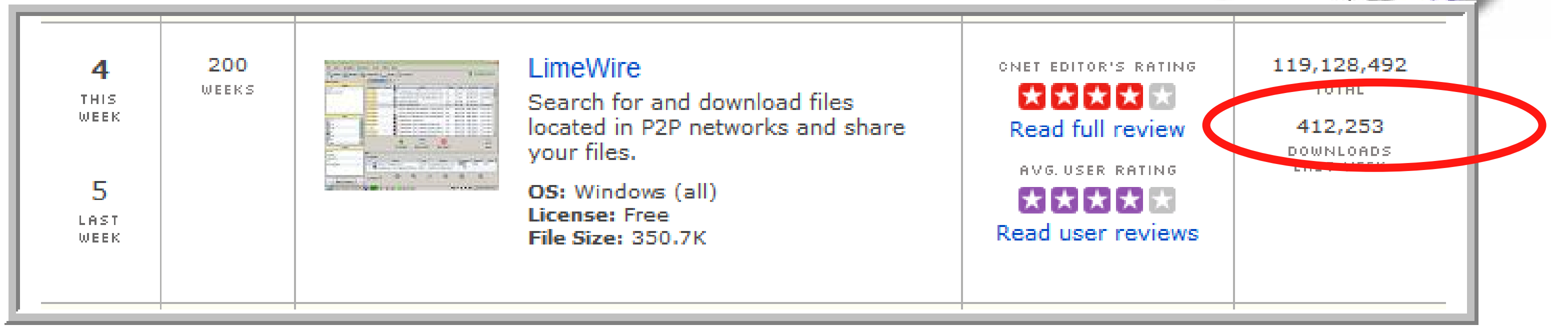
Monday, June 4, 2007

top overall searche

Leaders RSS

Rank		Prev	Subject	Move
1	↑	3	WWE (309)	+27
2	↑	10	NASCAR (107)	+104
3	↑	11	Limewire (26)	-
4	–	4	NBA (166)	-
5	↑	8	Spider-Man 3 (65)	
6	↑	12	RuneScape (309)	
7	↓	2	Lindsay Lohan (281)	
8	↑	9	Hi-5 (123)	
		22	Par	

c|net Most Popular Software Downloads



4 THIS WEEK 5 LAST WEEK	200 WEEKS	LimeWire Search for and download files located in P2P networks and share your files. **OS:** Windows (all) **License:** Free **File Size:** 350.7K	CNET EDITOR'S RATING ★★★★☆ Read full review AVG. USER RATING ★★★★☆ Read user reviews	119,128,492 TOTAL 412,253 DOWNLOADS LAST WEEK

WW P2P user captured searches related to *credit card*

- 2006 credit card numbers
- 2007 batch of credit cards
- 2007 credit card numbers
- a&l credit card
- aa credit card application
- abbey credit cards
- abbey national credit card
- ad credit card authorization
- april credit card information
- athens mba credit card payment
- atw 4m credit card application
- austins credit card info
- auth card credit
- authorization credit card
- authorization for credit card
- authorize net credit card
- bank and credit card informati
- bank credit card
- bank credit card information
- bank credits cards passwords
- bank numbers on credit cards
- bank of america credit cards
- bank of scotland credit card
- bank staffs credit cards only
- barnabys credit card personal
- bibby chase credit card
- bobs credit card
- bonnie credit card
- boost mobile credit card
- card auth credit
- card credit
- card credit numbers
- carl credit card
- cash credit card checks
- cathys visa credit card go on
- chase credit card
- chase credit card info
- chase freedom credit card
- cibc credit card vince
- citi credit card
- company credit cards
- confidential credit card app
- corperate credit card log
- credit and debit card
- credit card & online banking
- credit card acc numbers logins
- credit card acct numbers
- credit card activity
- credit card addresses phone
- credit card agreement
- credit card albert collins
- credit card and personal
- credit card ap info
- credit card app pdf
- credit card application
- credit card approved
- credit card approvel
- credit card aurthorization
- credit card auth
- credit card auth ctv
- credit card auth form
- credit card auth form cust
- credit card authorisation
- credit card authorisation july
- credit card authorization
- credit card bank info
- credit card bank numbers
- credit card batches
- credit card bills
- credit card charge ctm costa
- credit card charge request
- credit card comm sept private
- credit card confirmations
- credit card debit
- credit card gateway ubc
- credit card holders list
- credit card info on letterhead
- credit card information hotel
- credit card list
- credit card log
- credit card mastercard visa
- credit card merch copy sr
- credit card merchant
- credit card merchant info
- credit card names and numbers
- credit card number social
- credit card numbers and mercha
- credit card numbers personal
- dads bank info credit card
- davids credit card numbers
- dawns credit cards
- credit card payment doc
- credit card payment reciept
- credit card pin numbers
- credit card processing
- credit card reciepts
- credit card statements
- credit card status
- credit card stmt
- credit card tan cust copy sr
- credit card tan merch copy
- credit card transactions
- credit card visa
- credit card website access
- credit card wells fargo bill
- credit card with acc
- credit card with cv2 numbers
- credit cards banking online
- credit cards merchant numbers
- credit cards numbers visa
- credit cards social security
- credit cards statement fo may
- credit cards valids to visa cc
- credits cards passwords paypal
- d&b credit card info

- care office nbc health
- medicine mental health crc of
- hospital records
- mental hospitals
- hospital
- hospital letterhead
- hospital records
- niagara hospital
- american medical
- connolly medical ups prostate
- data entry medical billing fax
- dear medical insurance my
- denial of medical insurance
- hendee w r medical imaging
- isilo medical
- medical
- medical claims
- medical exam
- medical history
- medical passwords
- medical permission
- medical records certification
- medical release
- medical secretary cover letter
- medicine medical passwords
- authorization for medical
- authorization for medical of c
- authorization for medical of j
- authorizationform medical
- basic medical forms
- basic medical laboratory techn
- benny medical jack insurance
- billing medical

- billy connolly medical checkup
- billy connoly medical check
- canada medical test
- canadian medical
- canadian medical association
- canadian medical law
- caulfield general medical
- cbt6 citc1 medical expenses
- certficat medical
- certicat medical
- certifica medical
- certificat medical
- charlee medical costs
- charlee medical costs on the
- child medical exam
- child medical exams
- child medical release form
- cigna medical dr
- cigna medical drs
- classified medical records
- complete medical exam
- comprehensive medical
- compudoc medical
- computerize medical
- computerize medical billing tu
- computers in the medical offi
- computers medical doctors
- connelly medical check billy
- connelly medical ups
- billing medical august

- dear medical assurance my
- dear medical insurance my
- dear medical my assurance
- denial of medical insurance
- dental medical cross coding
- detective medical
- digital files medical trans
- distributeur medical
- doctor - medical checkup
- doctor fake medical by exam
- doctor medical exam
- Doctors medical billing
- doctors office medical exam
- doctors order medical doctor
- doctors orders medical
- doug medical bill
- doug stanhope medical pms
- edimis medical software 3.9
- electronic medical
- electronic medical record
- electronic medical record osx
- electronic medical record.pdf
- electronic medical records
- electronic medical systems
- electronics & bio medical
- emt medical software
- forms medical
- forms medical liability form
- forms medical office
- ge medical
- ge medical syatems
- medical coding and billing
- medical coding exam

- letter for medical bills
- letter for medical bills dr
- letter for medical bills etmc
- letter re medical bills 10th
- ltr client medical report
- ltr hjh rosimah medical
- ltr medical body4life
- ltr medical maternity portland
- ltr medical misc portland
- ltr orange medical head center
- ltr to valley medical
- lytec medical billing
- medical investigation
- medical journals password
- medical .txt
- medical abuce records
- medical abuse
- medical abuse records
- medical algoritms
- medical authorization
- medical authorization form
- medical autorization
- medical benefits
- medical benefits plan chart
- medical biliing
- medical biling
- medical bill
- medical biller resume
- medical billig software
- medical billing
- medical billing windows

How often are fraud / ID theft terms searched?

Credit Card

55,823 times

- Credit Cards with cv2 numbers
- April credit card information
- Bank of America credit cards

Credit

117,965 times

- Credit reports
- Credit score
- Credit report barbara

Credit Card Brands*

75,571 times

- Citibank mastercard richard
- Hacked visa credit cards
- Discover card id number

* Visa, Mastercard, Amex, Discover

Source: Tiversa search monitoring for period Aug 16 – Aug 29, 2007

How often are fraud / ID theft terms searched?

Tax Return

49,904 times

- Tax return irs & state checks
- Tax returns efile doc
- Lewis tax return

Account

34,921 times

- Online account
- Rapidshare premium accounts
- Paypal account

Quicken Brands*

55,650 times

- Quicken accounting
- Quickbooks point of sale
- Quickbooks crack

* Quicken, Quickbooks

Source: Tiversa search monitoring for period Aug 16 – Aug 29, 2007

How often are fraud / ID theft terms searched?

Medical

82,598 times

- cbt6 citc1 medical expenses
- dear medical insurance my
- hendee w r medical imaging

Password & PIN

317,338 times

- Usernames passwords to bank
- Online passwords
- Passwords txt

Credit Check Brands*

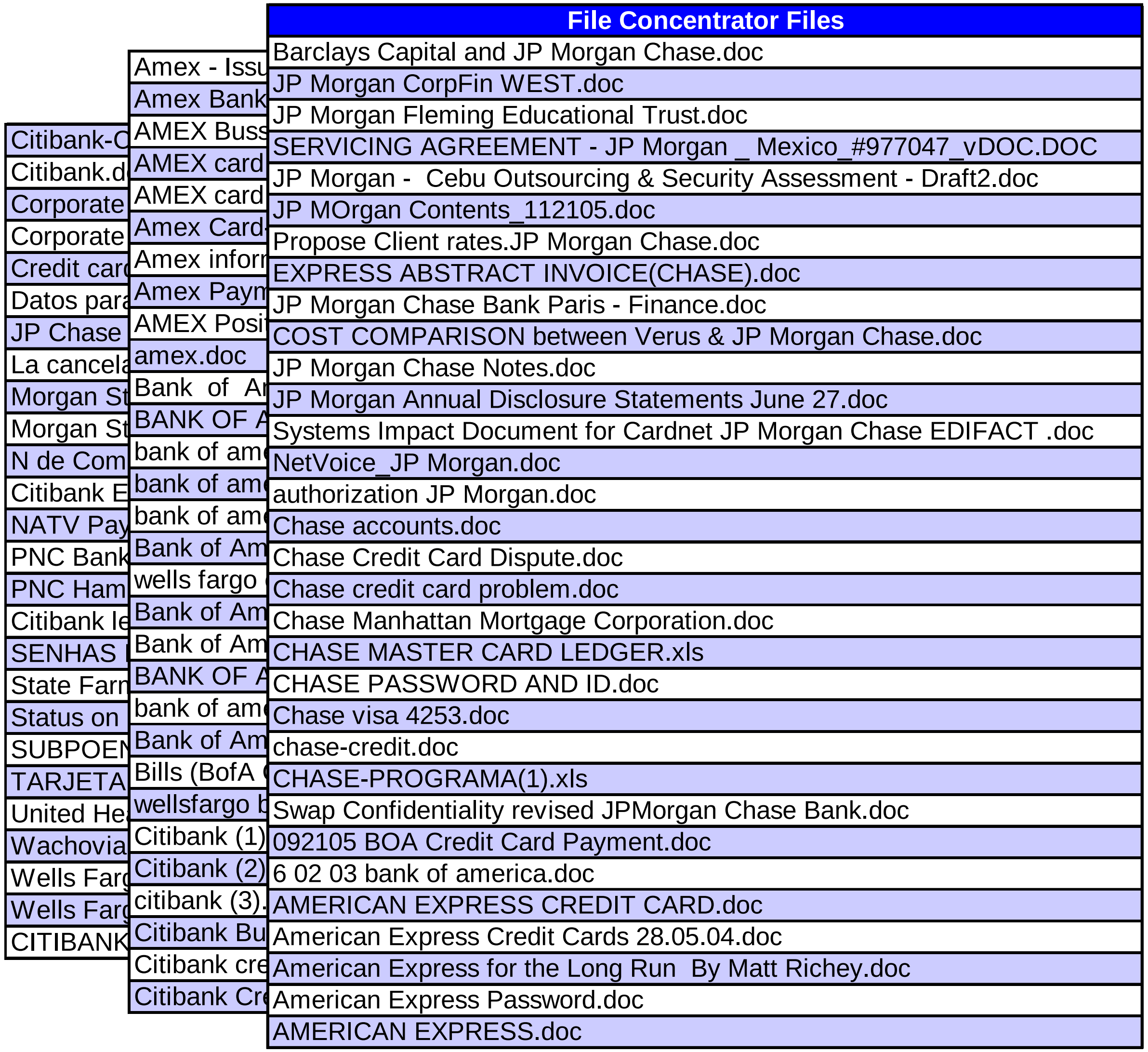
4,115 times

- Equifax consumerdec
- Annualcreditreport experian
- Dougs credit report equifax in

* Equifax, Experian, Transunion

Source: Tiversa search monitoring for period Aug 16 – Aug 29, 2007

File Concentrators collect files from these searches…



Citibank-C
Citibank.d
Corporate
Corporate
Credit card
Datos para
JP Chase
La cancela
Morgan St
Morgan St
N de Com
Citibank E
NATV Pay
PNC Bank
PNC Ham
Citibank le
SENHAS
State Farn
Status on
SUBPOEN
TARJETA
United He
Wachovia
Wells Farg
Wells Farg
CITIBANK

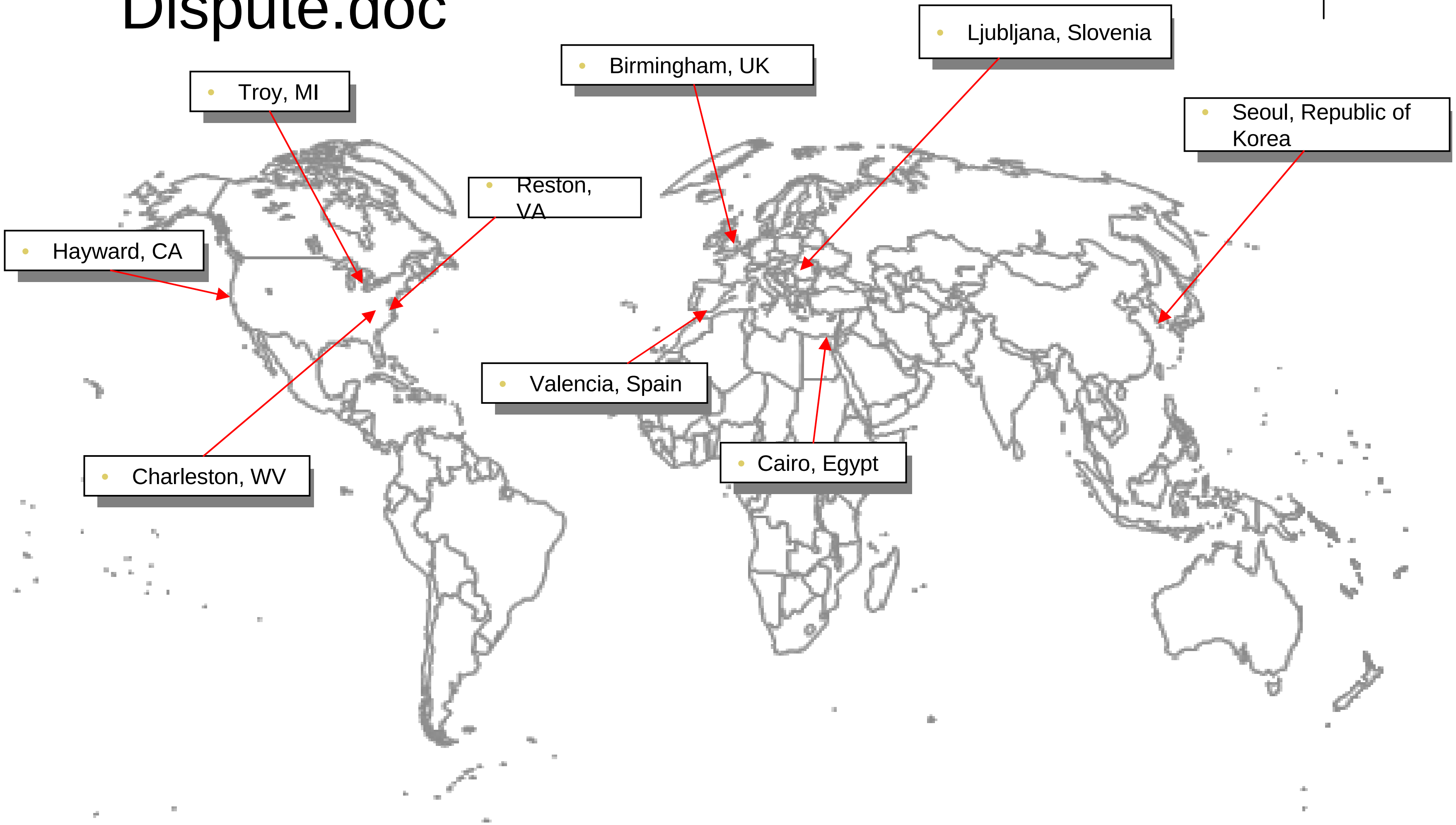
Amex - Issu
Amex Bank
AMEX Buss
AMEX card
AMEX card
Amex Card
Amex inforr
Amex Payn
AMEX Posi
amex.doc
Bank of Ar
BANK OF A
bank of ame
bank of ame
bank of ame
Bank of Am
wells fargo
Bank of Am
Bank of Am
BANK OF A
bank of ame
Bank of Am
Bills (BofA
wellsfargo b
Citibank (1)
Citibank (2)
citibank (3).
Citibank Bu
Citibank cre
Citibank Cre

File Concentrator Files
Barclays Capital and JP Morgan Chase.doc
JP Morgan CorpFin WEST.doc
JP Morgan Fleming Educational Trust.doc
SERVICING AGREEMENT - JP Morgan _ Mexico_#977047_vDOC.DOC
JP Morgan - Cebu Outsourcing & Security Assessment - Draft2.doc
JP MOrgan Contents_112105.doc
Propose Client rates.JP Morgan Chase.doc
EXPRESS ABSTRACT INVOICE(CHASE).doc
JP Morgan Chase Bank Paris - Finance.doc
COST COMPARISON between Verus & JP Morgan Chase.doc
JP Morgan Chase Notes.doc
JP Morgan Annual Disclosure Statements June 27.doc
Systems Impact Document for Cardnet JP Morgan Chase EDIFACT .doc
NetVoice_JP Morgan.doc
authorization JP Morgan.doc
Chase accounts.doc
Chase Credit Card Dispute.doc
Chase credit card problem.doc
Chase Manhattan Mortgage Corporation.doc
CHASE MASTER CARD LEDGER.xls
CHASE PASSWORD AND ID.doc
Chase visa 4253.doc
chase-credit.doc
CHASE-PROGRAMA(1).xls
Swap Confidentiality revised JPMorgan Chase Bank.doc
092105 BOA Credit Card Payment.doc
6 02 03 bank of america.doc
AMERICAN EXPRESS CREDIT CARD.doc
American Express Credit Cards 28.05.04.doc
American Express for the Long Run By Matt Richey.doc
American Express Password.doc
AMERICAN EXPRESS.doc

- File Concentrators collect & ‘concentrate’ files of value
- File Concentrators exhibit “suspicious intent”
- Tiversa observes *thousands* of such individuals on the WW P2P
- This Example: 92 separate files held by one individual

…share them…

- File diffusion – Chase Credit Card Dispute.doc

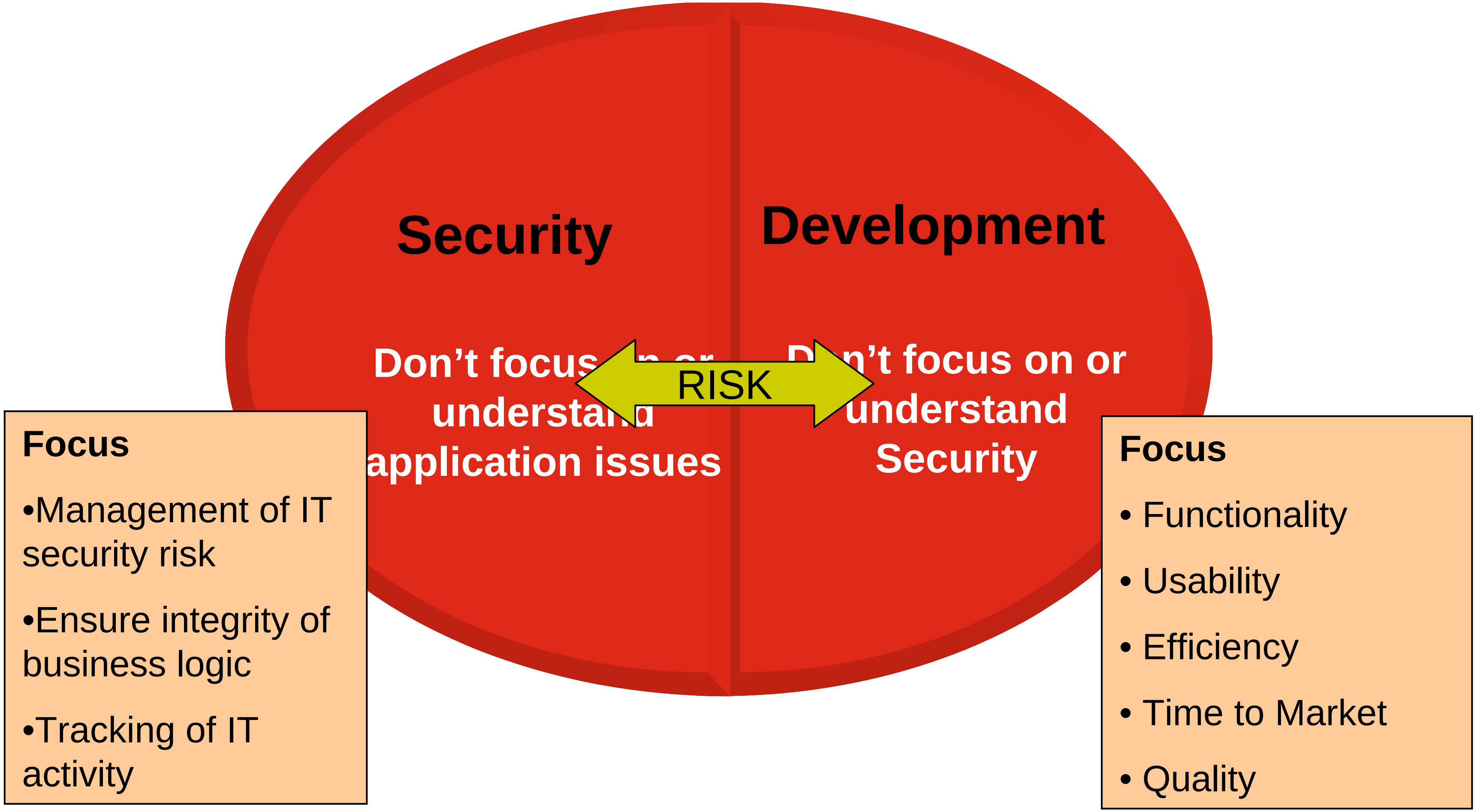


- Troy, MI
- Birmingham, UK
- Ljubljana, Slovenia
- Seoul, Republic of Korea
- Reston, VA
- Hayward, CA
- Valencia, Spain
- Charleston, WV
- Cairo, Egypt

Application Security- Security is Not Quality!

- Although a small (very small) number of security issues overlap with quality problems:
  - **Both high quality and low quality software can have security issues**
  - **Quality is cumulative - 80-20 rule applies**
  - **Security is absolute - 20% of doors unlocked is not secure**
  - **Quality problems are reported by end users, often with great details**
  - **Security problems are found after the fact, often with little information to recreate**

Application Security Gap



Security
Development
Don't focus on or understand application issues
RISK
Don't focus on or understand Security

Focus

- Management of IT security risk
- Ensure integrity of business logic
- Tracking of IT activity

Focus

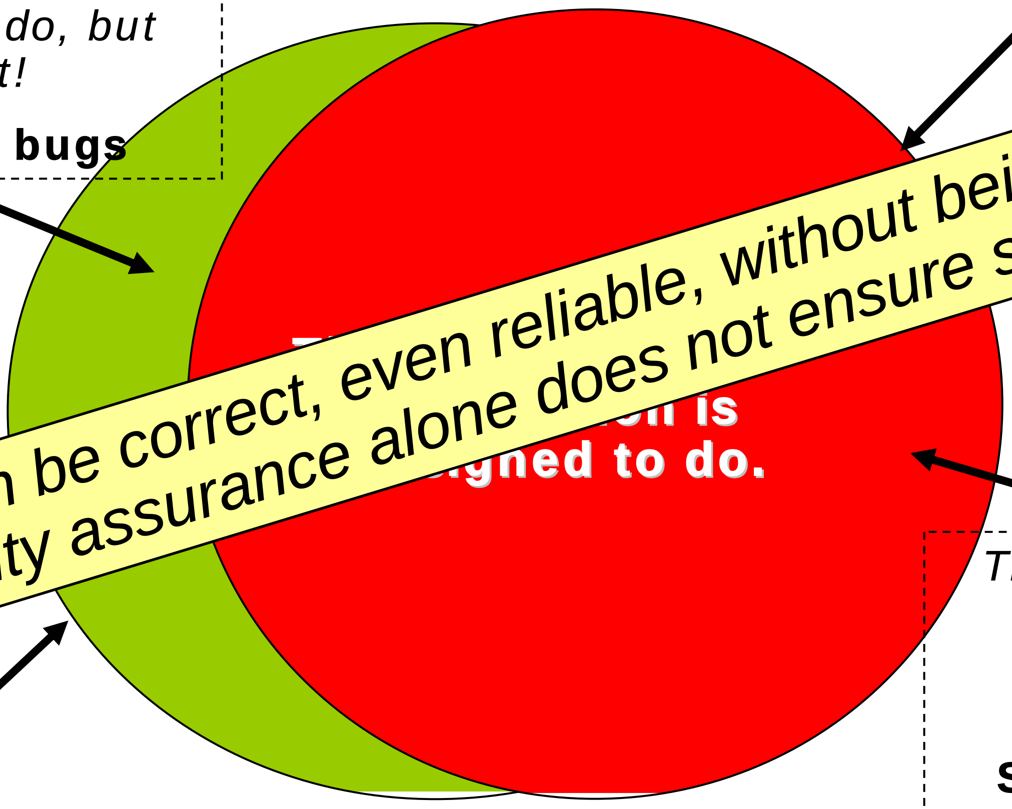
- Functionality
- Usability
- Efficiency
- Time to Market
- Quality

The Result…

The application as developed.

This is what your application was supposed to do, but doesn't!

Functionality bugs



Software can be correct, even reliable, without being secure — quality assurance alone does not ensure security

This is what your application CAN do, but you're not aware of.

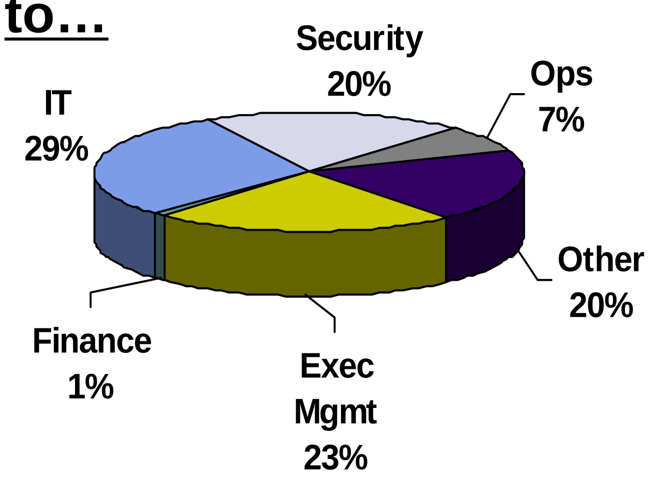
Security flaws

The application as designed.

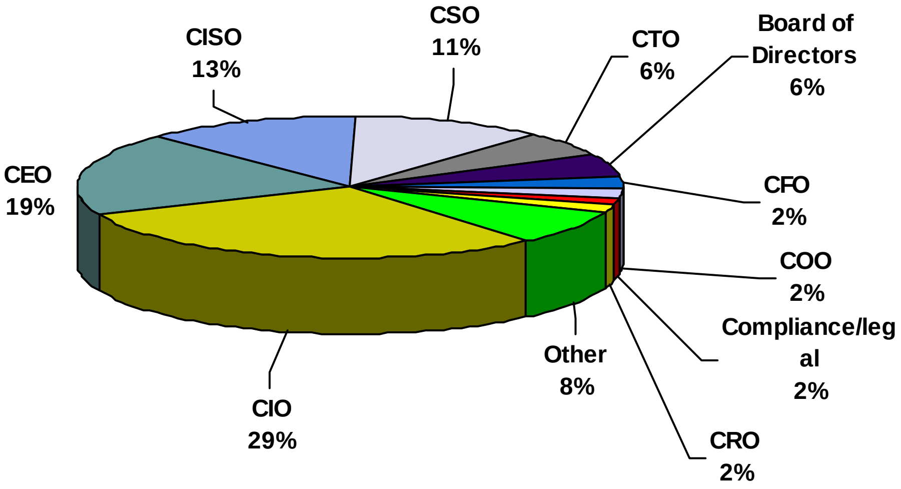
Security Department Structure

- *A slight increase in the percentage reporting into Exec management and a slight decrease in reporting into IT demonstrates the criticality of Info security in today's environments*

IS Professional Reports to…



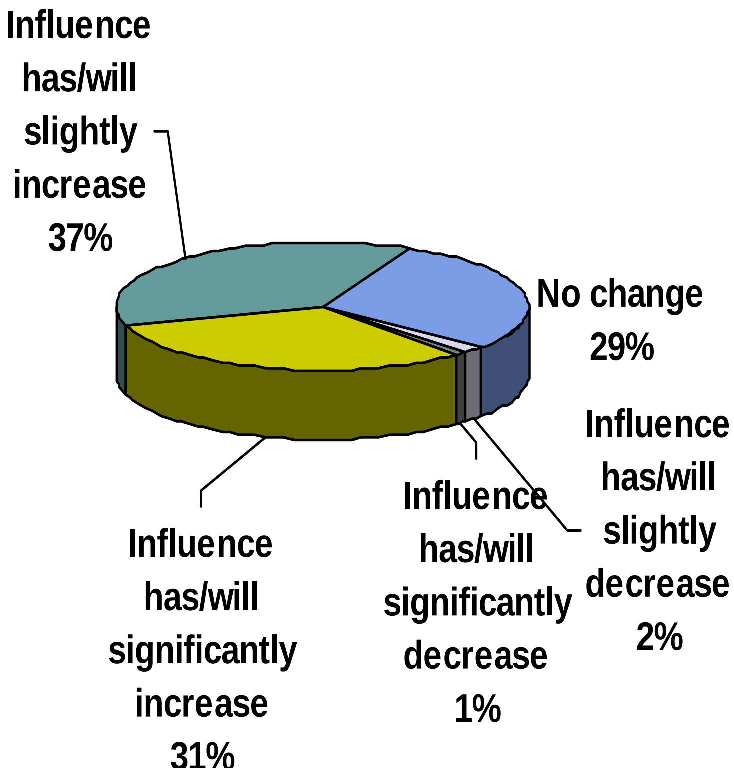
- **Ultimate Accountability for Info Security…**



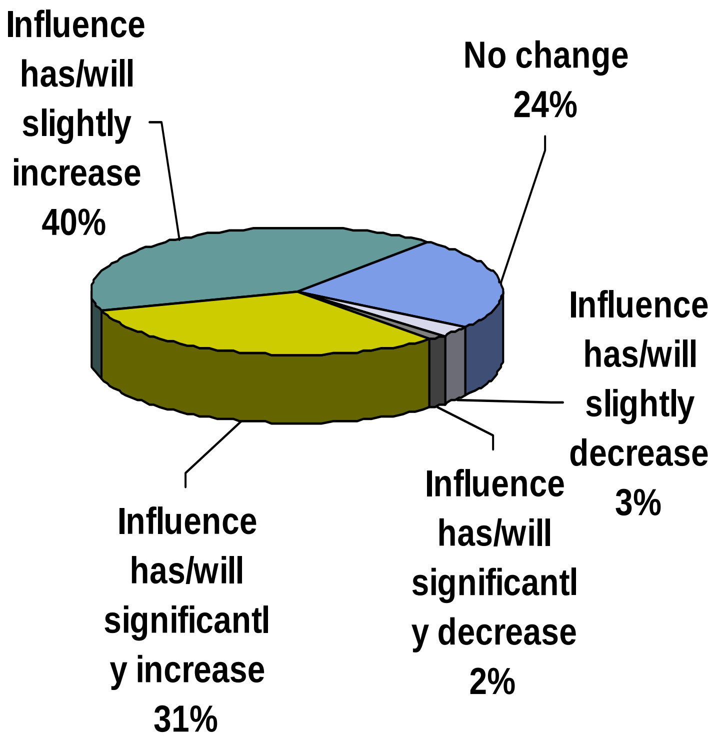
Source: IDG 2006 Global Information Security Workforce Study

Information Security – Level of influence within Business Units & at Exec level

In the past 12 months



- ## In the next 12 months



Source: IDG 2006 Global Information Security Workforce Study

Important Elements in Effectively Securing Infrastructure

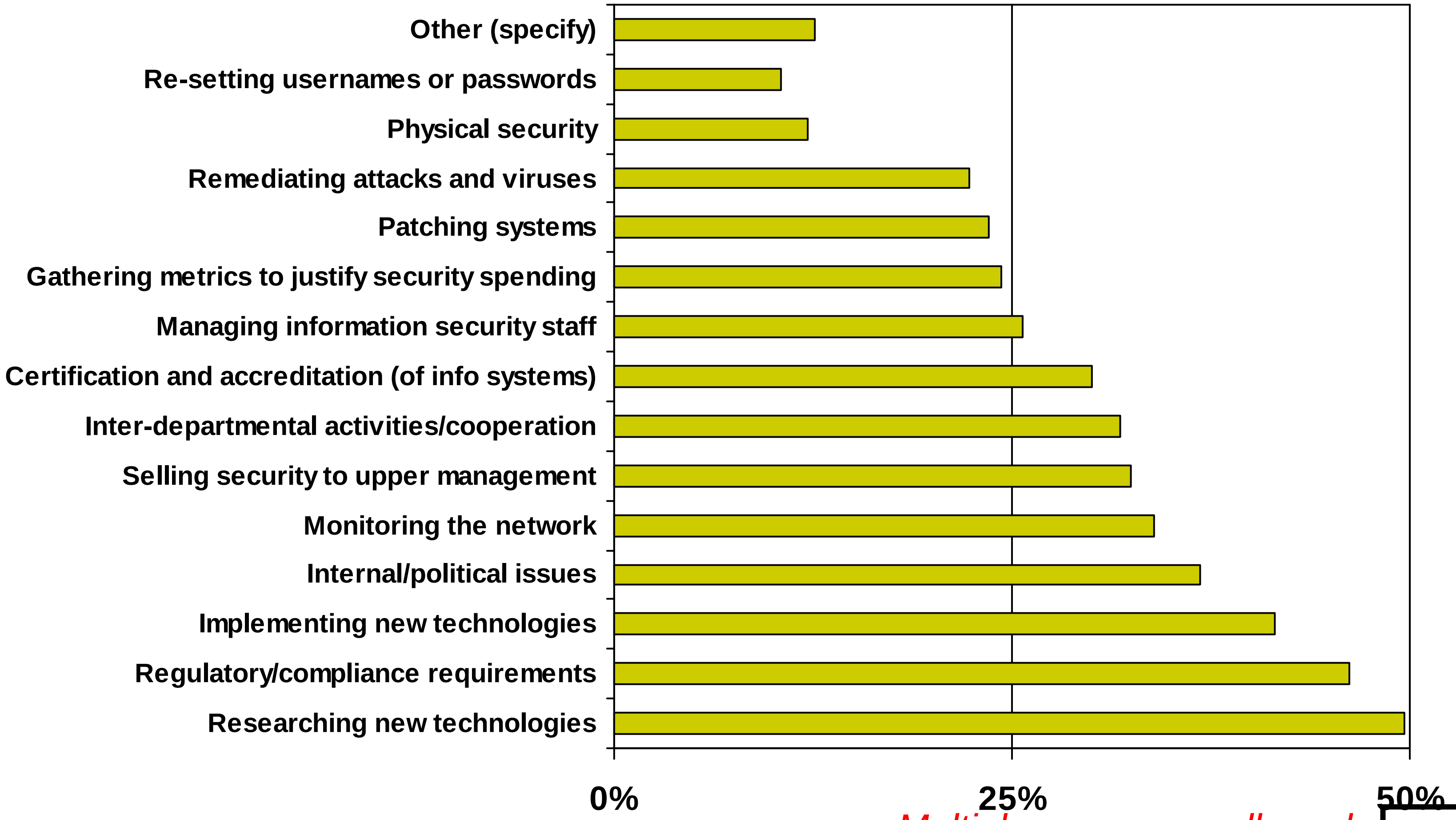
People including management are very important!!

	Most Important	2nd most important	3rd most important	4th most important	Least Important
Hardware solutions	**11%**	**9%**	**10%**	**22%**	**48%**
Software solutions	**8%**	**15%**	**14%**	**45%**	**18%**
Qualified security staff	**19%**	**22%**	**40%**	**10%**	**9%**
Users **following security policy**	**19%**	**34%**	**23%**	**14%**	**10%**
Management **support of security policies**	**43%**	**21%**	**13%**	**9%**	**15%**
N	3852	3858	3866	3865	3784

Source: IDG 2006 Global Information Security Workforce Study

Activities Identified as Consuming a Significant Portion of Security Professional's Time

Not only technical but management aspects consuming their time!



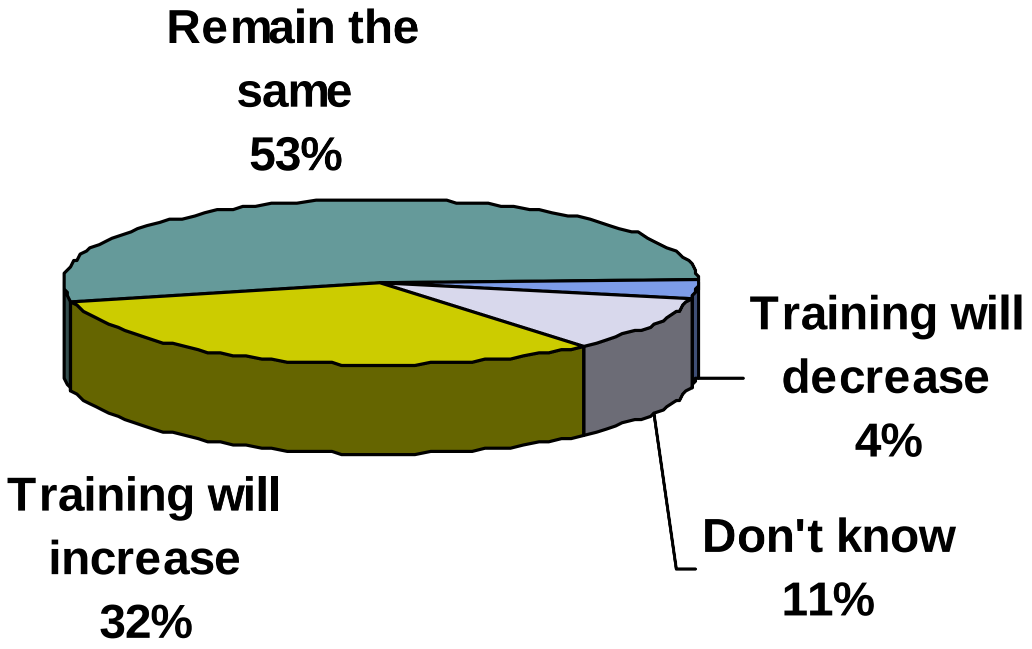
Multiple responses allowed

N = 3861

Source: IDG 2006 Global Information Security Workforce Study

Training for Information Security Professionals

- In 2007, training for information security professionals will…



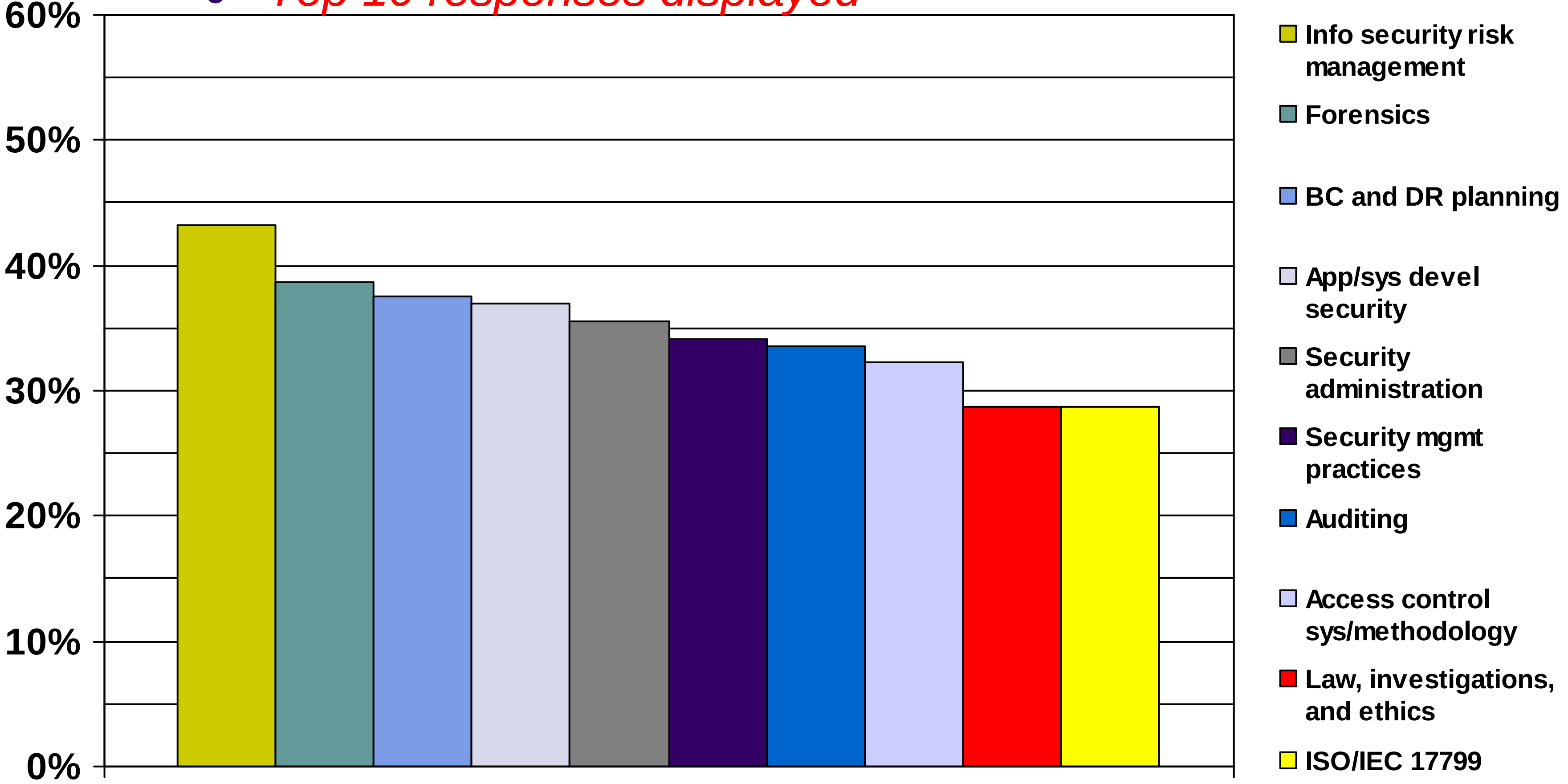
- *If an increase is expected, the increase will be nearly 30%*

Source: IDG 2006 Global Information Security Workforce Study

Demand Areas for Training and Certification

Not one specific area but multiple knowledge/sill are required!!

- *Top 10 responses displayed*



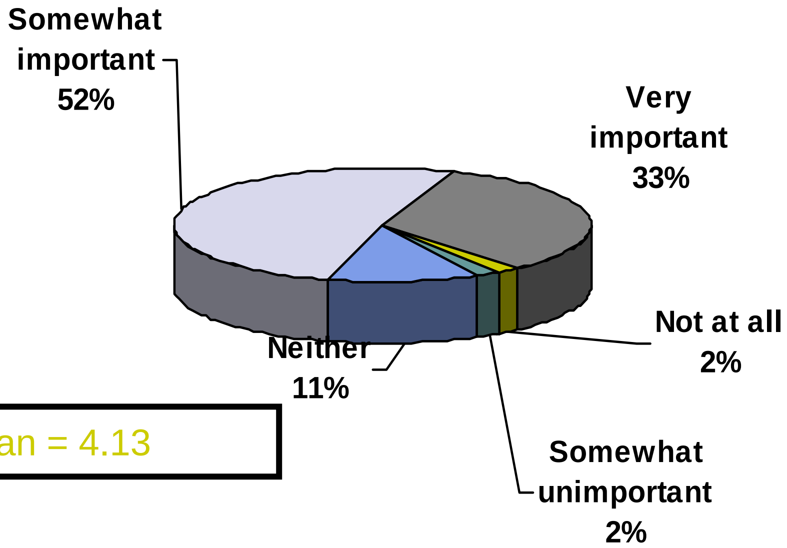
Source: IDG 2006 Global Information Security Workforce Study

N = 3763

Importance of Security Certifications

- *33% of respondents are responsible for making hiring decisions for Information security staff*

- Importance of Security Certifications when hiring security staff…



Mean = 4.13

- Reasons to Hold Certifications…

Employee competence	67%
Quality of work	59%
Company policy	33%
Regulatory requirement	27%
Legal/due diligence	21%
DoD Directive 8570.1	12%
Other	5%

- *85% believe that security certifications are either somewhat important or very important when making hiring decisions for information security staff*

Source: IDG 2006 Global Information Security Workforce Study

N = 2653

Summary

- IT security becoming integral part of the risk management and compliance of the organization
- Threats becoming more complex and global
  - Wireless, ID Theft, Application security
- Influence of IT security has increased, and organization starts recognize “People” is the key!
- Not only technology but management aspects of knowledge and skills are required for IT security staff
- Education AND certification is considered very important to raise people and evaluate people

It's the People!