The Easiest Score on the Internet

FIRST Conference

Vancouver, BC

June 26, 2008

Agenda

- The Problem
- Solutions
- Questions

Agenda

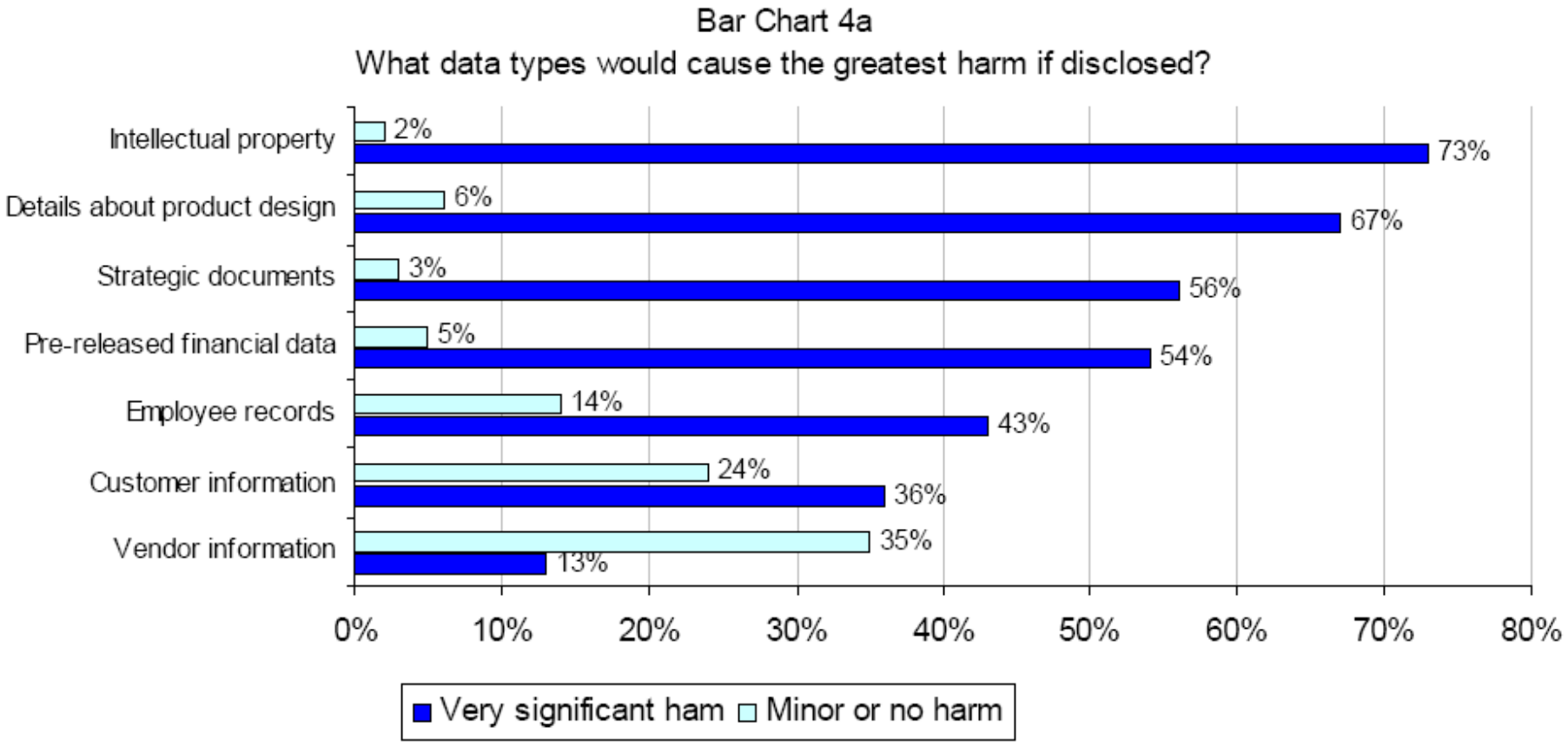
- **The Problem**
- Solutions
- Questions

What if you knew…

- …that sensitive and confidential documents regarding your organization were publicly available on the internet?
- …that the source of these documents were not only your employees, but your vendors, partners, and even customers?
- …that internet users are actively searching for these documents by name?
- …that criminals, the media, competitors, and foreign governments use these documents and profit from them?

…what would you or could you do?

What type of "leaked" data would cause the greatest harm?



Source: Ponemon Institute – Ignored Crisis in Data Security: P2P File Sharing

Publicly available confidential files found on P2P – what would you do if on a corporate web site?

Human Resources

- Performance reviews
- Salary histories
- Retained recruiter interview write-ups
- Termination rationale / detailed record
- Sexual harassment case write-ups
- Employee PII lists (SS#'s, salaries)

Marketing & PR

- Multi-year internal advertising plans
- Product launch plans and estimated sales targets
- Copy / story boards for commercials
- Press releases in mark-up before release
- Multi-year public relations and marketing plan

Legal

- Non-disclosure agreements
- Master service agreements
- Patent applications
- Documents in anticipation of litigation
- Letters of intent
- Documents marked attorney / client privilege
- Bad debt recovery legal documents

Executive

- Board meeting minutes
- Board of directors confidential contact lists
- Results of SARBOX compliance studies
- Merger / acquisition plans & financials
- Executives' travel itineraries, tail numbers, driver contacts, etc.
- Executives' home addresses, personal cell, home, and e-mail addresses
- Term sheets
- Letters of intent

Customer

- Dispute letters
- User ID / Password Lists
- Trust Documents
- Account statement screen captures
- Mortgage applications
- Bank account applications
- Wire transfer authorizations
- Credit report copies
- Online banking transaction screen captures
- Bad debt recovery documents
- Scanned credit cards
- Tax returns

Sales

- Responses to RFI's / RFP's
- Internal prices lists and hourly rate sheets
- Internal sales meeting presentations
- Customer lists and identifying information
- Client contact lists with e-mail, phone numbers, etc.
- Client meeting minutes exposing client identities and conversations
- Invoices and purchase orders

Physical Security

- New facility HVAC, electrical, security plans
- Physical security audits showing vulnerability points
- Guard schedules with contact information
- Branch bank daily hour-by-hour physical security procedures
- ATM cash withdrawal procedures and access codes
- Employee itineraries, events, locations, tail numbers, driver numbers, etc.
- Building blue prints / floor maps

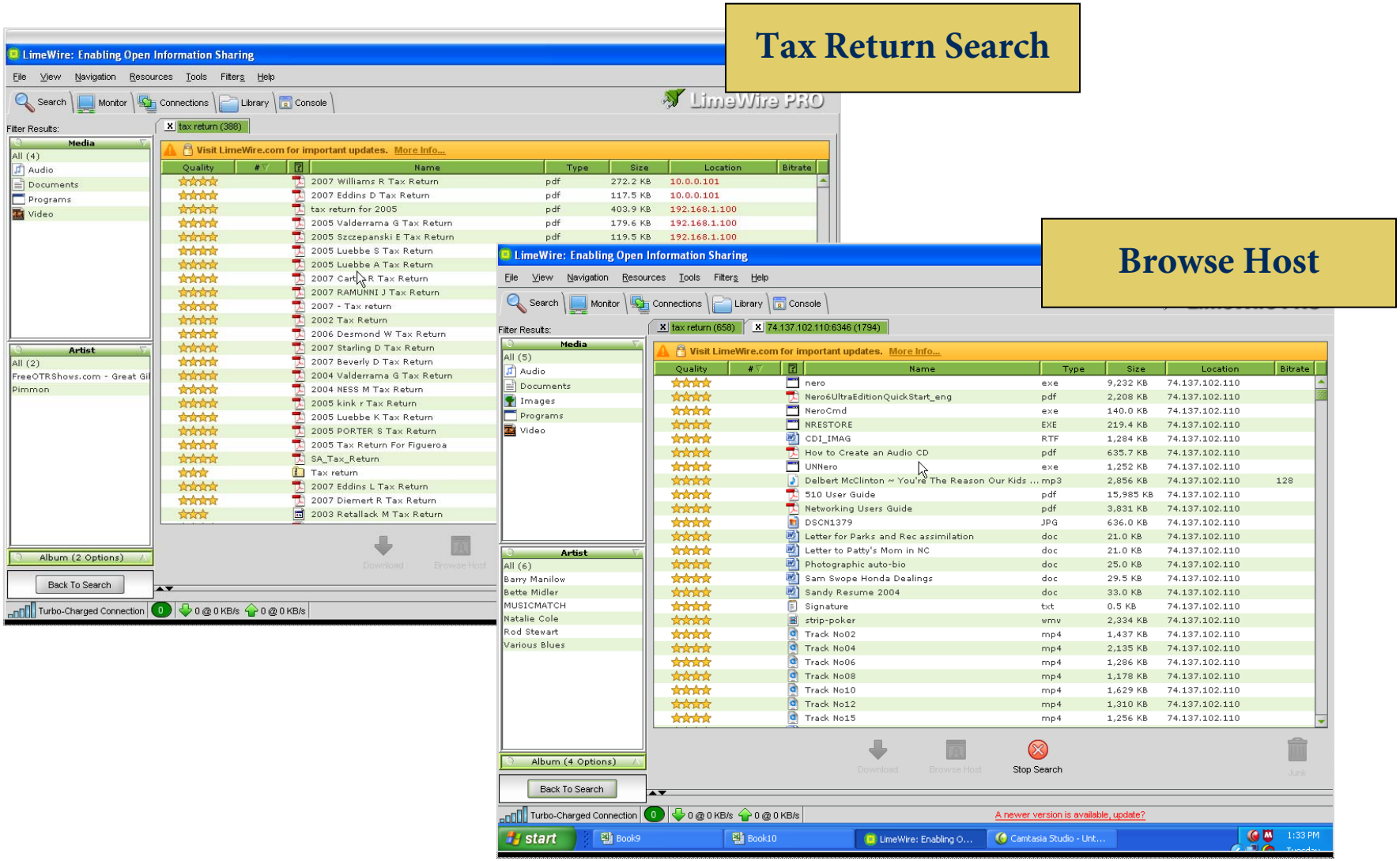
Information Technology

- Disaster recovery procedures/plans
- Mainframe login/passwords
- WAN, Intranet, VPN user id / passwords
- Encryption keys
- Computer code specifications & architecture plans
- IT project plans with scope of work, deadlines, and contacts
- Network diagrams
- IT Acceptable Use Policies (w/ P2P policy)

Operations & Security

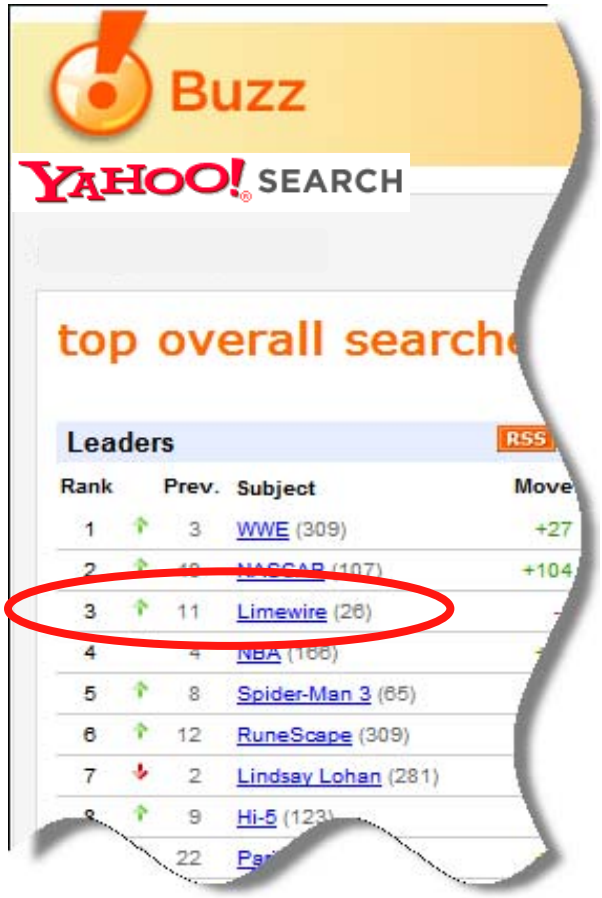
- Customer account lists with visible P.I.I
- Call center call log records w/ high net worth customer P.I.I.
- Client files processed by Spanish to English translator
- RFPs, RFQs with highly sensitive corporate plans indicated
- Conference call numbers with access codes for internal meetings
- Invoices and purchase orders
- Customer account lists
- Pricing and hourly rates paid to vendors

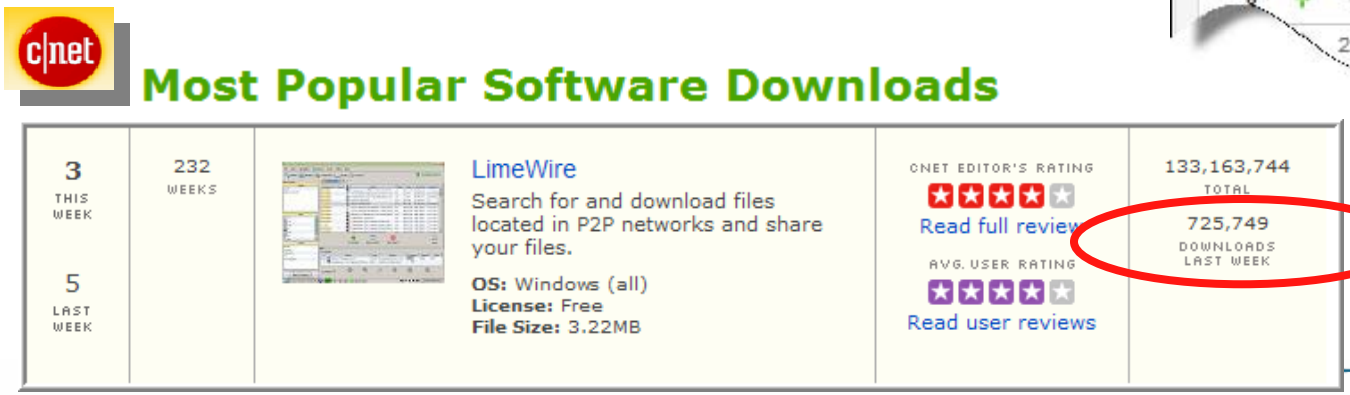
Individual P2P User Experience – Tax Return Search



The worldwide (WW) P2P is large and rapidly growing

- Over 1.5 billion searches a day – larger than Google (133 million)
- Over 450 million copies of filesharing software
- Over 20 million unique users a day
- Over 65% of internet bandwidth
- LimeWire is on over 30% of world's computers alone

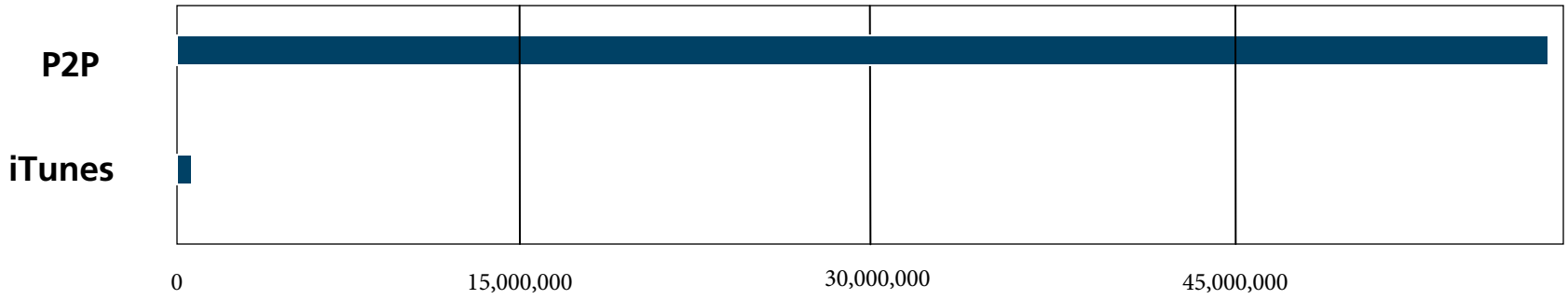




P2P volume compared to World Wide Web

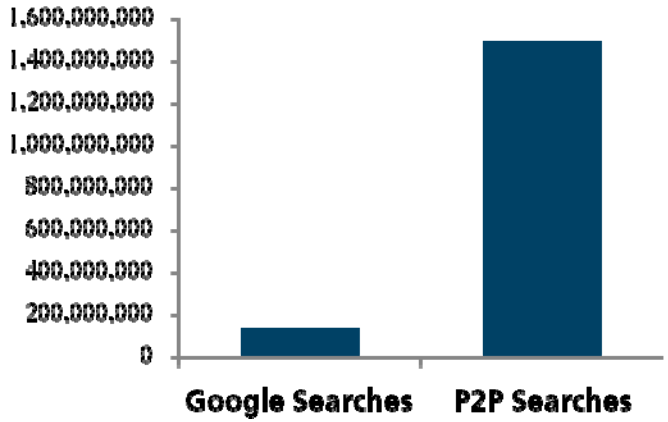
Songs Acquired on iTunes and P2P During second half 2007

(000)



Source: RIAA, Apple, FTI

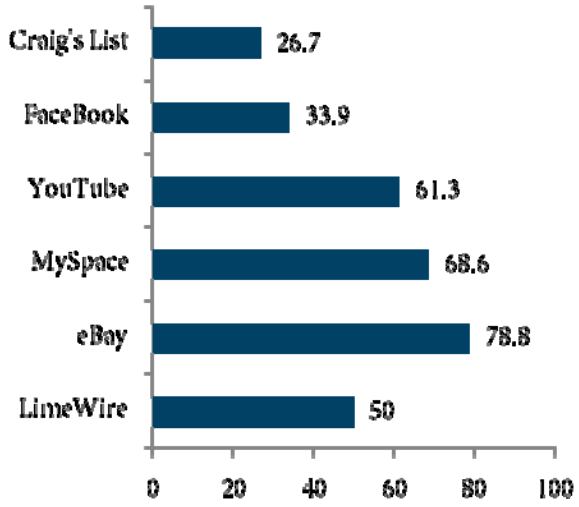
Internet Searches Processed – Web versus P2P – November 2007



Source: Nielson Net Ratings; Tiversa

Unique Monthly Users

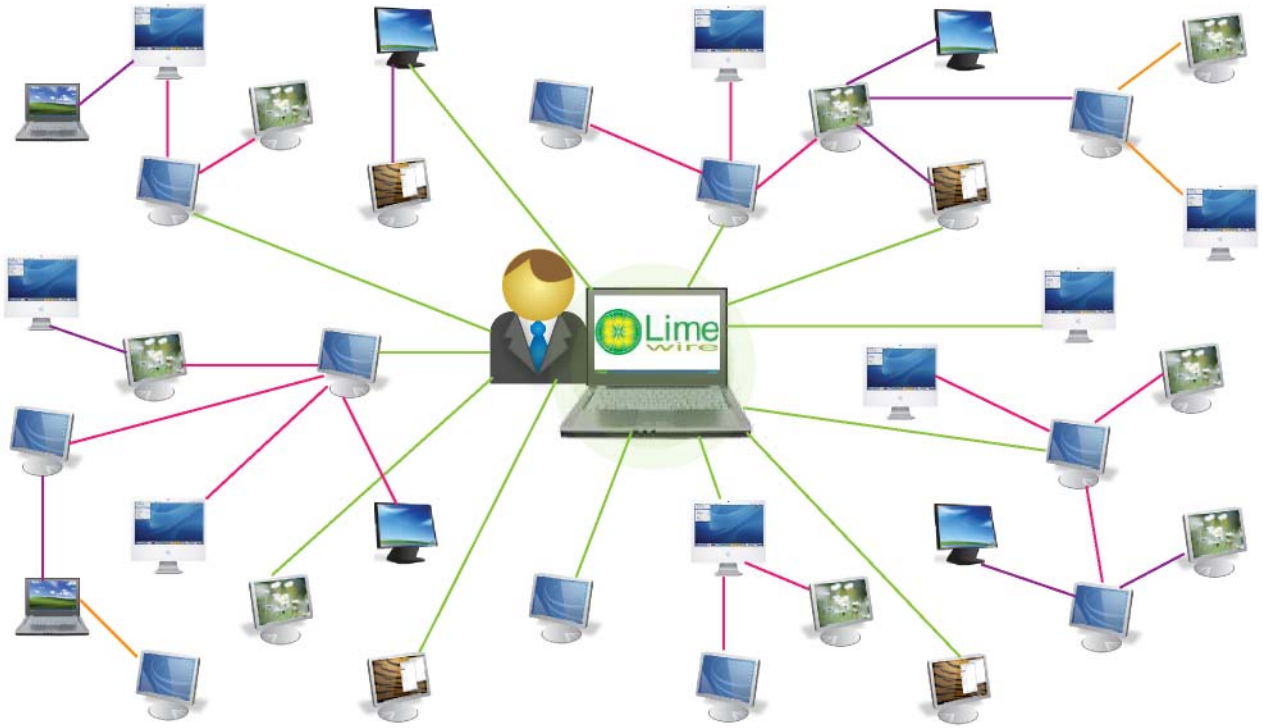
MM



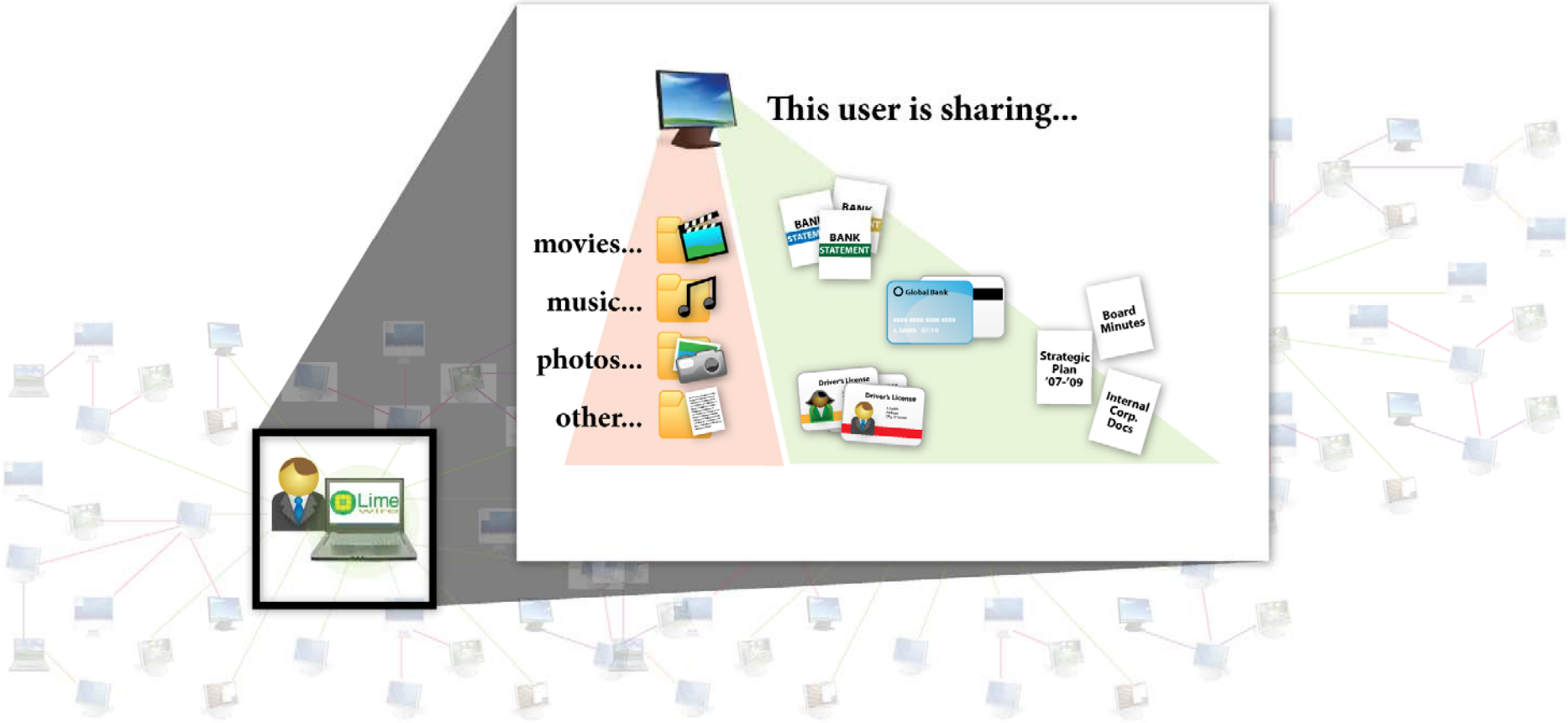
Source: ComScore Jan 08, LimeWire

What is peer-to-peer file sharing?

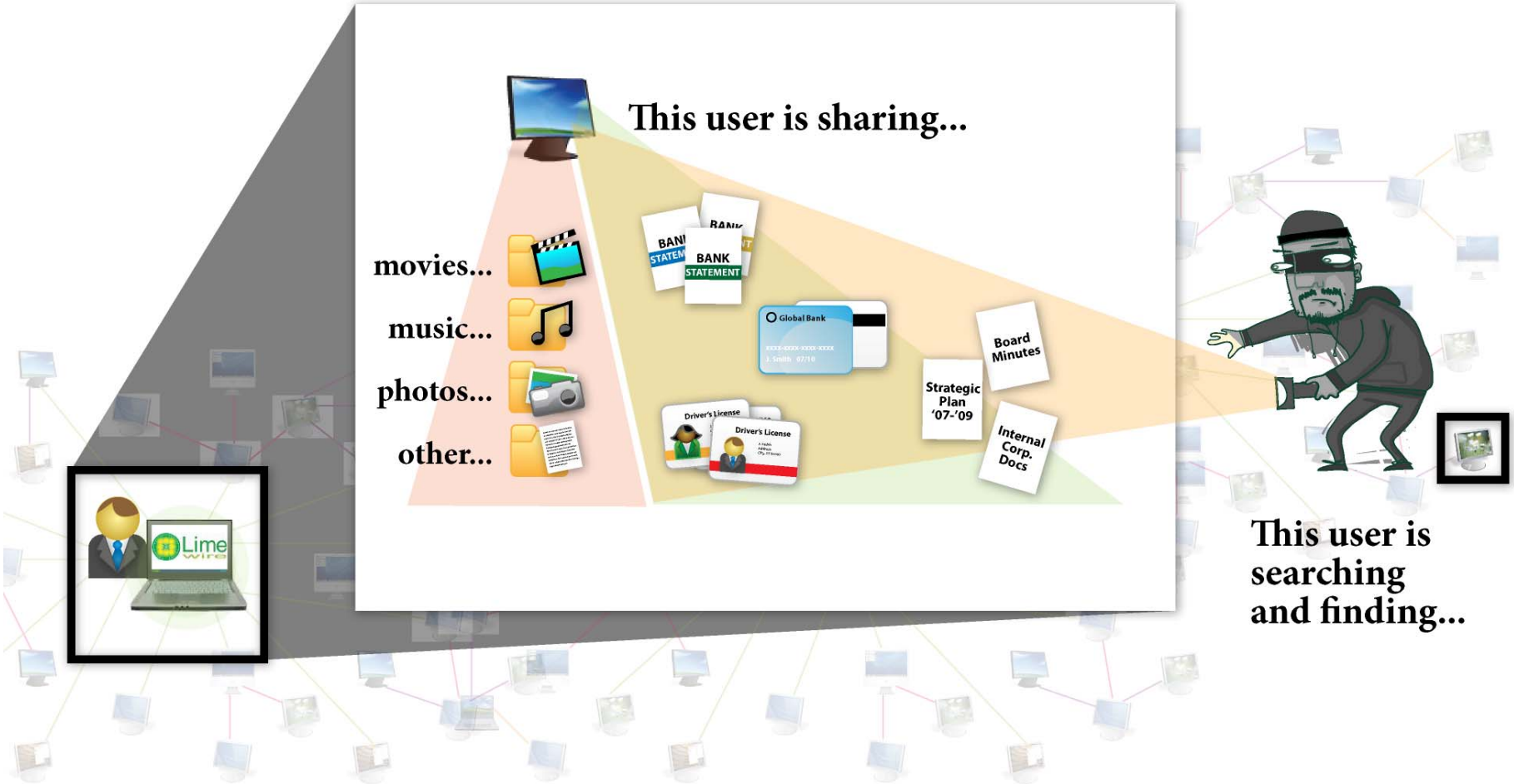
What is peer-to-peer file sharing?



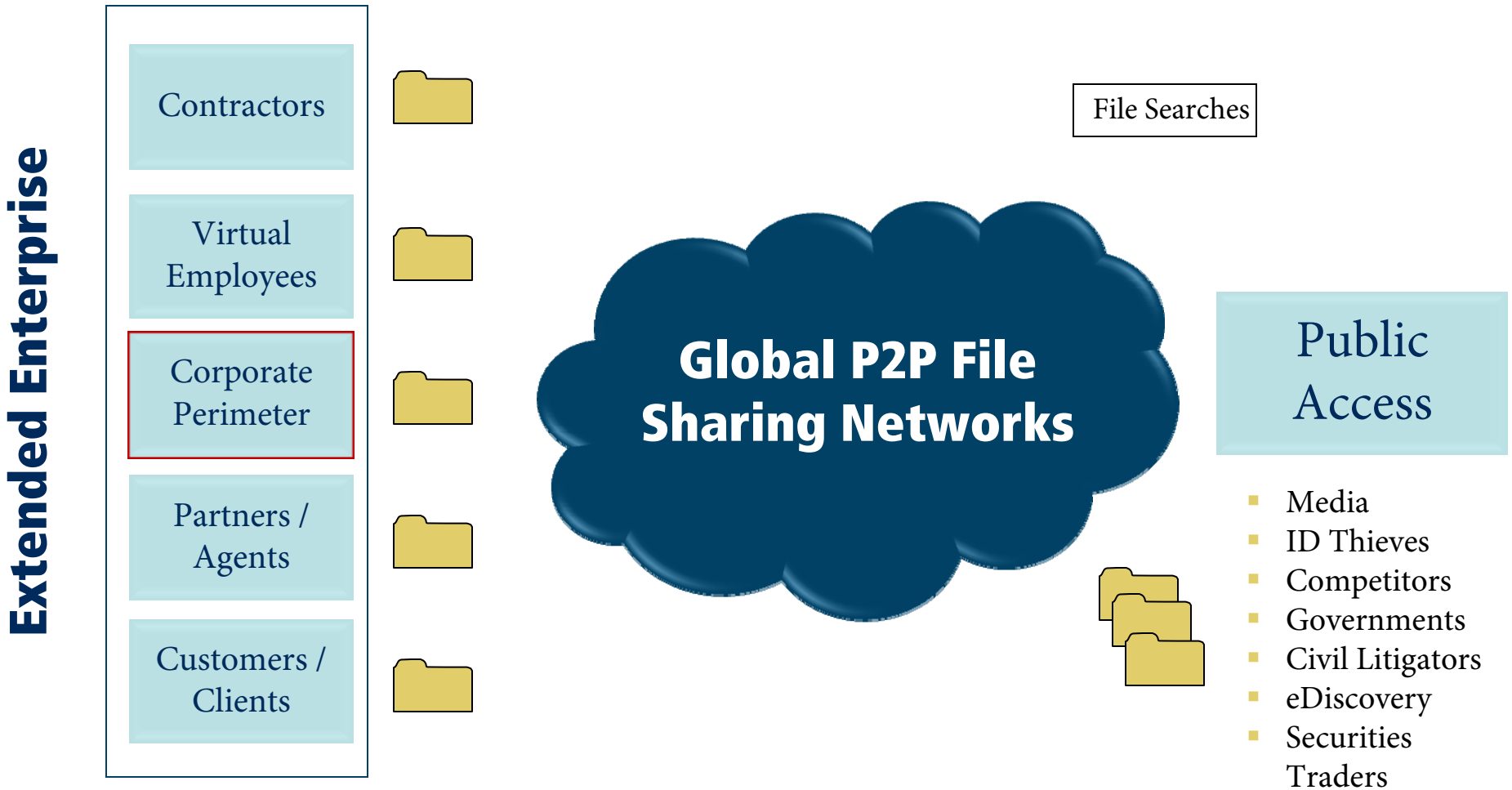
What is peer-to-peer file sharing?



What is peer-to-peer file sharing?

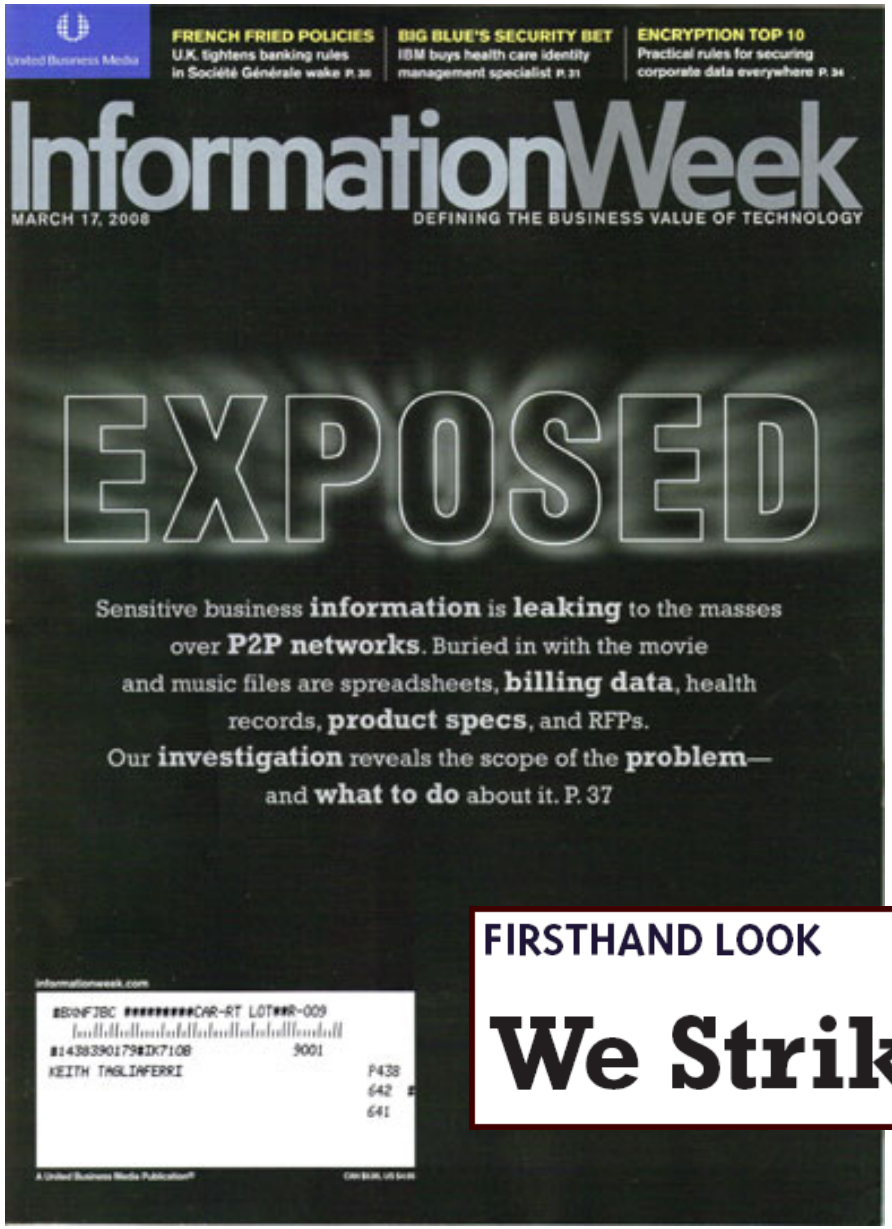


The *Extended Enterprise* creates P2P disclosure risk



TIVERSA

Information Week article clearly highlights the problem



InformationWeek
Research & Reports

FIRSTHAND LOOK

IN DEPTH / P2P DATA LEAKS

We Strike Data Galore

TIVERSA

Recent publicly disclosed P2P disclosures….

Affected Organization	Date Public	Discovered By	Disclosure Source	Exposed
Pfizer	May/June 2007	Company	Employee at Home	17,000 Current & Former Employees' Social Security and Personal Data
Citigroup	September 2007	Reporter	Employee at Home	5,000 Mortgage Customers' Social Names and Social Security Numbers
U.S. Dept. of Transportation	May 2007	Reporter	Chief Privacy Officer at Home	66 DOT and National Achieve Documents
Federal Transit Authority	September 2007	Reporter	Files belonged to Booz-Allen	Confidential Terrorist Threat Assessments on Chicago and 34 Others Cities
NewFoundland – Labrador Gov't	February 2008	Private Investigator	Contractor	694 files Affecting 153 People – Names, Medical Histories, etc.
Walter Reed Army Hospital	June 2008	3rd Party	Physician	1,000 patient records

Other cases…dodged bullets

1. 10,840 credit card user's PII, current litigation, and public company financials coming from employee's home computer
2. Almost 2,500 individual W2 forms in one file coming from its own network
3. Current *Intrusion Detection System* technical plans for one of world's largest wireless phone carriers released by a contractor
4. All 4,250 employees names, salaries, and ethnic status disclosed by small HR contractor for public company
5. 52,345 credit card numbers, names, addresses, FICO scores, credit limits from bank in middle east exposing multiple royal family members
6. Almost 800 prominent Washington DC attorneys names, DOB, released by investment advisor
7. The user ID's and passwords for ***every*** critical system for ***brand name*** global healthcare center released by volunteer
8. Technical test results for space based laser system released by US Government Contractor

Source: notable disclosures – one week at Tiversa

TIVERSA

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
- blaww debt credit cards
- bobs credit card
- bonnie credit card
- boost mobile credit card
- brightstar credit card form
- 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

P2P user captured searches for the term - *medical*

- 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
- billing medical august
- 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
- 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

Information concentrator map

Information Concentrator Locations Found and Reported to a Financial Services Clients by Tiversa in 2007**

** Red pin represents individuals who have amassed consumer and corporate banking files with malicious intent

TIVERSA

Gift card taken and used by fraudsters to purchase prepaid cell phone

50.00 gift card

Glen Breakwater
506 Sonoma Dr.
Valrico, Fl 33594
813 643-4593

(For Emergencies Only)

Glen's $50 Visa Gift Card
4007-6617-7367-7509 CVV 143
Expires 03/09

metroPCS.
Unlimit Yourself.

Attempt 1
Dec 27 12:24
$60.00 - Declined

Attempt 2
Dec 27 12:24
$50.00 - Approved

Attempt 3
Dec 27 12:27
$30.00 - Declined

Global uptake of gift card "bait" test

Source: *Glen – Credit Card Number.doc*

Red Pins represent 23 P2P Taker Locations*

* File taken from (1) PC running file sharing software with file "Glen – Credit Card Numbers.doc" in shared directory

Tiversa Client authorized "bait" test

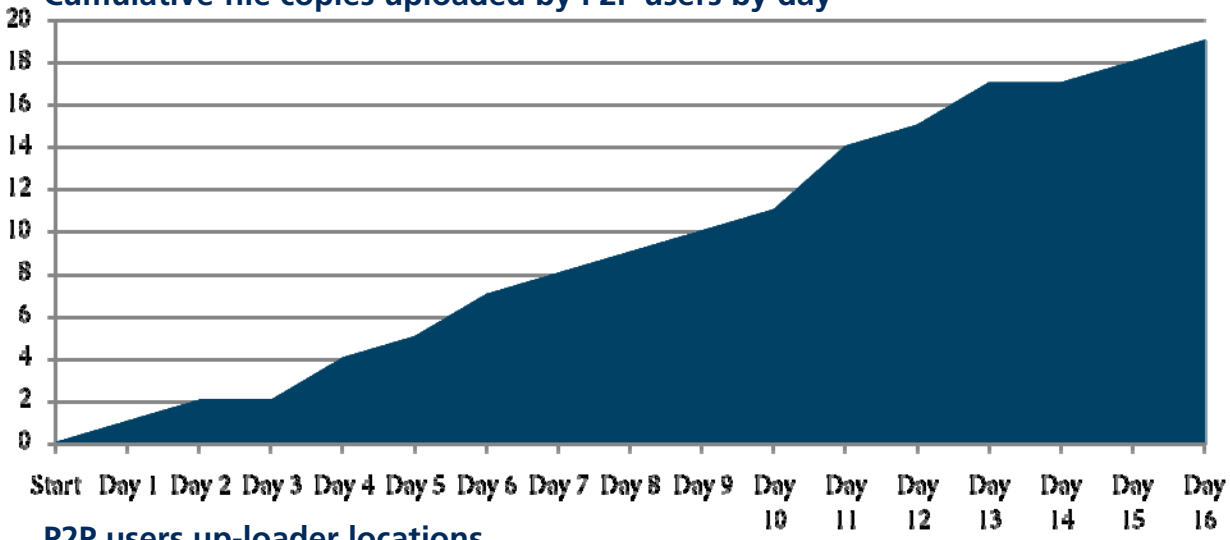
1. *Perimeter_Host_Credentials.xls*
2. *[Redacted]_Network_Perimeter.pdf*

Red Pins represent unique Taker Locations*

- 2 files taken 45 times
- 2 days

"Bait" test for IT related documents

Cumulative file copies uploaded by P2P users by day



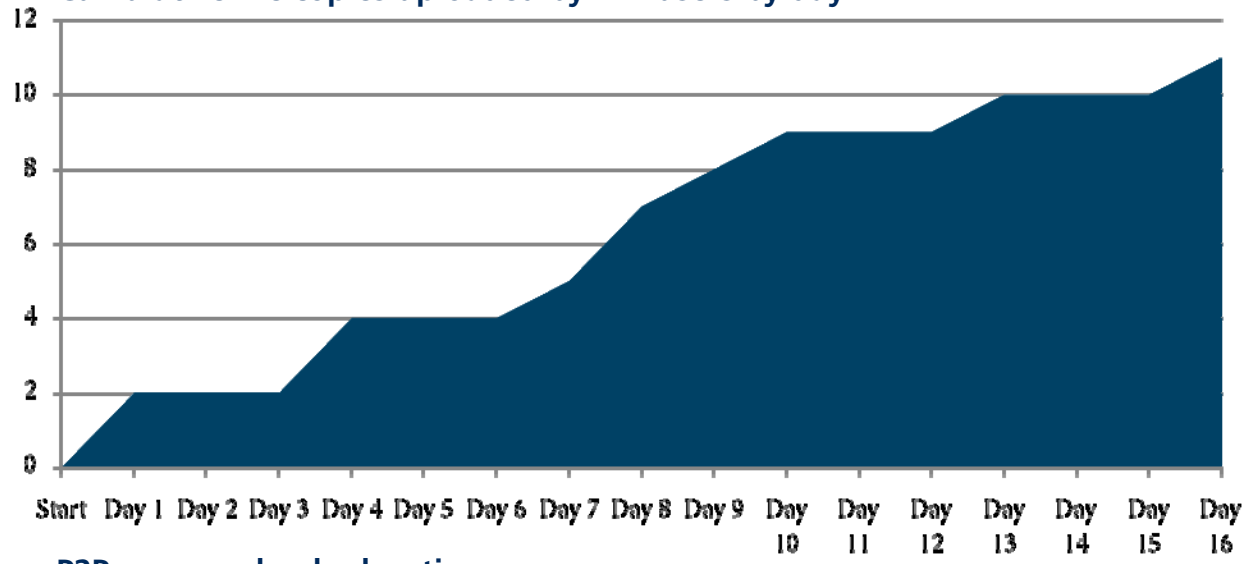
P2P users up-loader locations

- Bait File Name: *America Bank - CONFIDENTIAL IT Network Infrastructure.doc*
- Uploaded 19 times by 19 unique individuals
- 19 individuals located in 9 different countries on 5 continents

TIVERSA

"Bait" test for HR related documents

Cumulative file copies uploaded by P2P users by day

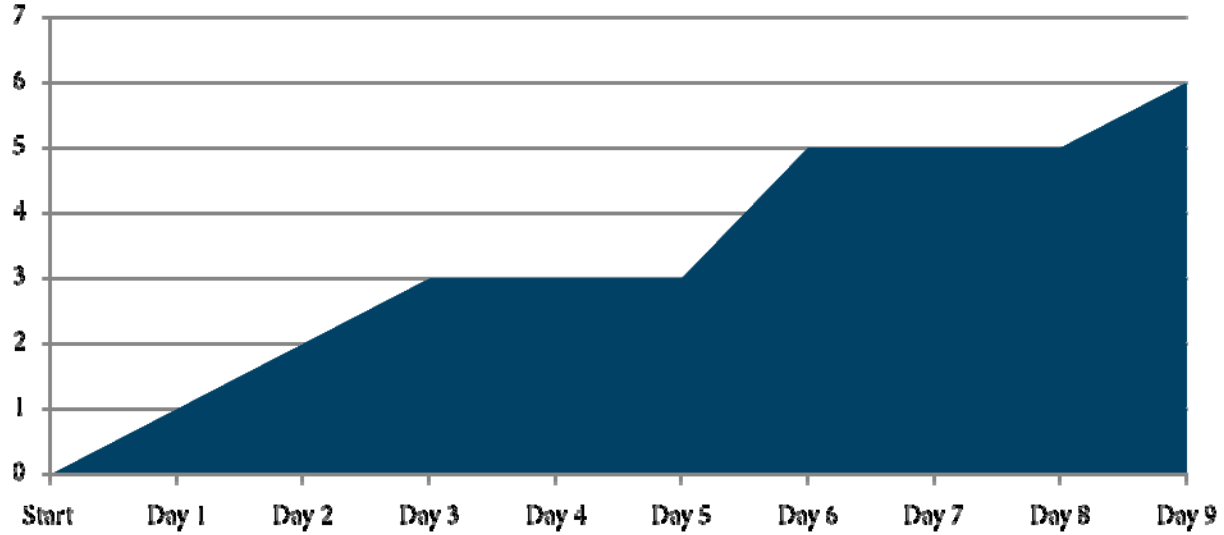


P2P users up-loader locations

- Bait File Name: *Claims_Purchasing_HR_Records_Output.xls*
- Uploaded 11 times by 11 unique individuals
- 11 individuals located in 8 different countries on 4 continents

"Bait" test for executive related documents

Cumulative file copies uploaded by P2P users by day



P2P users up-loader locations

- Bait File Name: *Alaska Bank - Board Minutes - INTERNAL ONLY.doc*
- Uploaded 6 times by 6 unique individuals
- 6 individuals located in 5 different countries on 3 continents

TIVERSA

"Bait" test for SIPRNET PASSWORDS

Source: *SIPRNET Passwords.doc*

Red Pins represent 12 resharer locations

* File taken from (1) PC running file sharing software with file "SIPRNET Passwords.doc" in shared directory. File did not contain actual SIPRNET information.

Kopiloff indictment case illustrates what malicious individuals do with information collected…

Section B(9) - Essence of the Scheme and Artifice to Defraud

The essence of the scheme and artifice to defraud was that GREGORY THOMAS KOPILOFF would use several methods, including the use of P2P file sharing networks afforded by ***LimeWire and Soulseek***, to:

1. surreptitiously and illicitly obtain identity, and also banking, financial, or credit information belong to others;
2. that KOPILOFF would then use the identity and also banking, financial, or credit information that belonged to others, without their knowledge or consent, to fraudulently obtain credit accounts in the names of others;
3. that KOPILOFF would then fraudulently obtain credit accounts in the names of others;
4. that KOPILOFF would then fraudulently purchase merchandise "online," also in the names of others and using the credit accounts he had fraudulently opened in their names;
5. that KOPILOFF would instruct the vendors of that merchandise to ship it to addresses designated by KOPILOFF where he, or an accomplice, would then receipt it;
6. and that KOPILOFF would then sell the merchandise at a substantial discount to other buyers; after which KOPILOFF would convert the proceeds from the sale of the fraudulently purchased merchandise to his own personal use and benefit.

Source: Case 07-CR-00309-INDI

P2P is more productive and gets richer information than phishing

Rates in Underground Market for PII

Source: Symantec

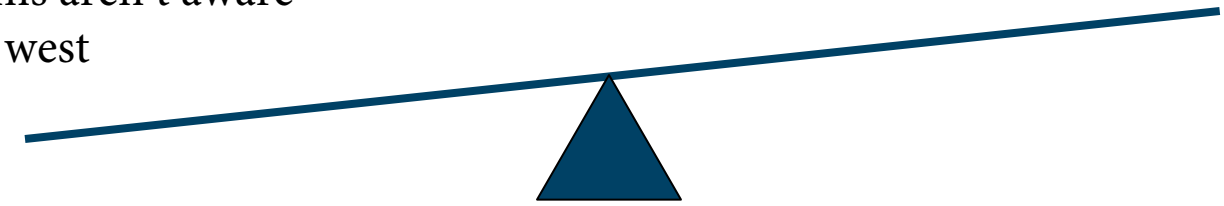
Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50 - $5
2	Bank Accounts	21%	$30 - $400
3	Email passwords	8%	$1 - $350
4	Mailers	8%	$8 - $10
5	Email Addresses	6%	$2/MB - $4/MB
6	Proxies	6%	$0.50 - $3
7	Full Identity	6%	$10 - $150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5 - $7
10	Compromised Unix Shells	2%	$2 - $10

P2P

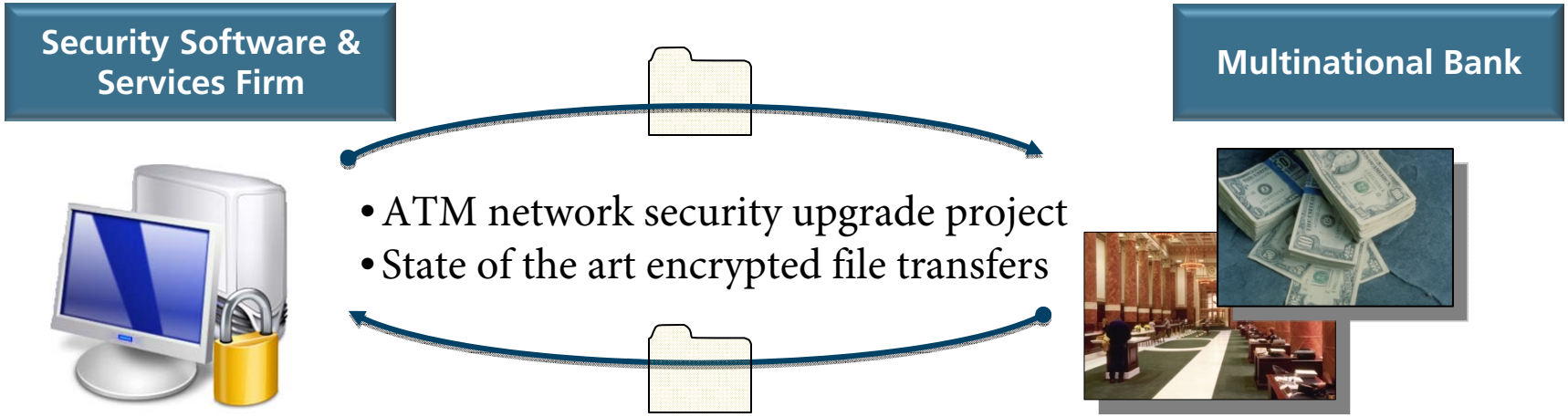
- Easy, low tech
- Don't have to trick anyone
- Dense, rich PII data per "hit"
- *Bonus:* Intellectual Property
- Victims aren't aware
- Wild west

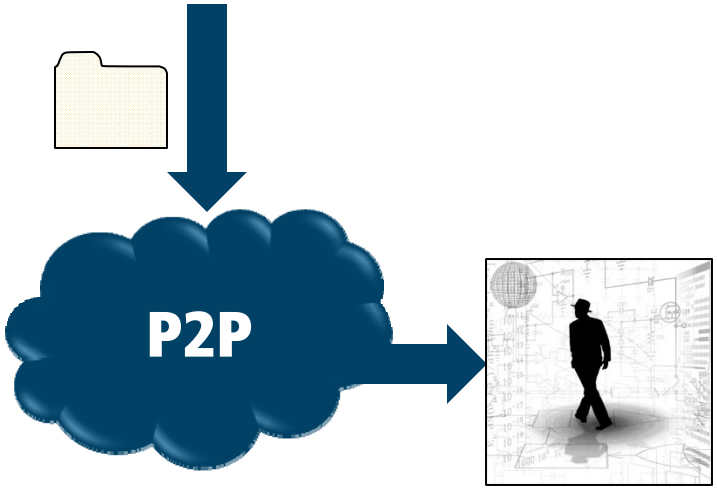
Phishing

- Difficult, requires tech
- Elaborate trick schemes
- One number at a time
- Victims notified
- Industry aimed at protecting



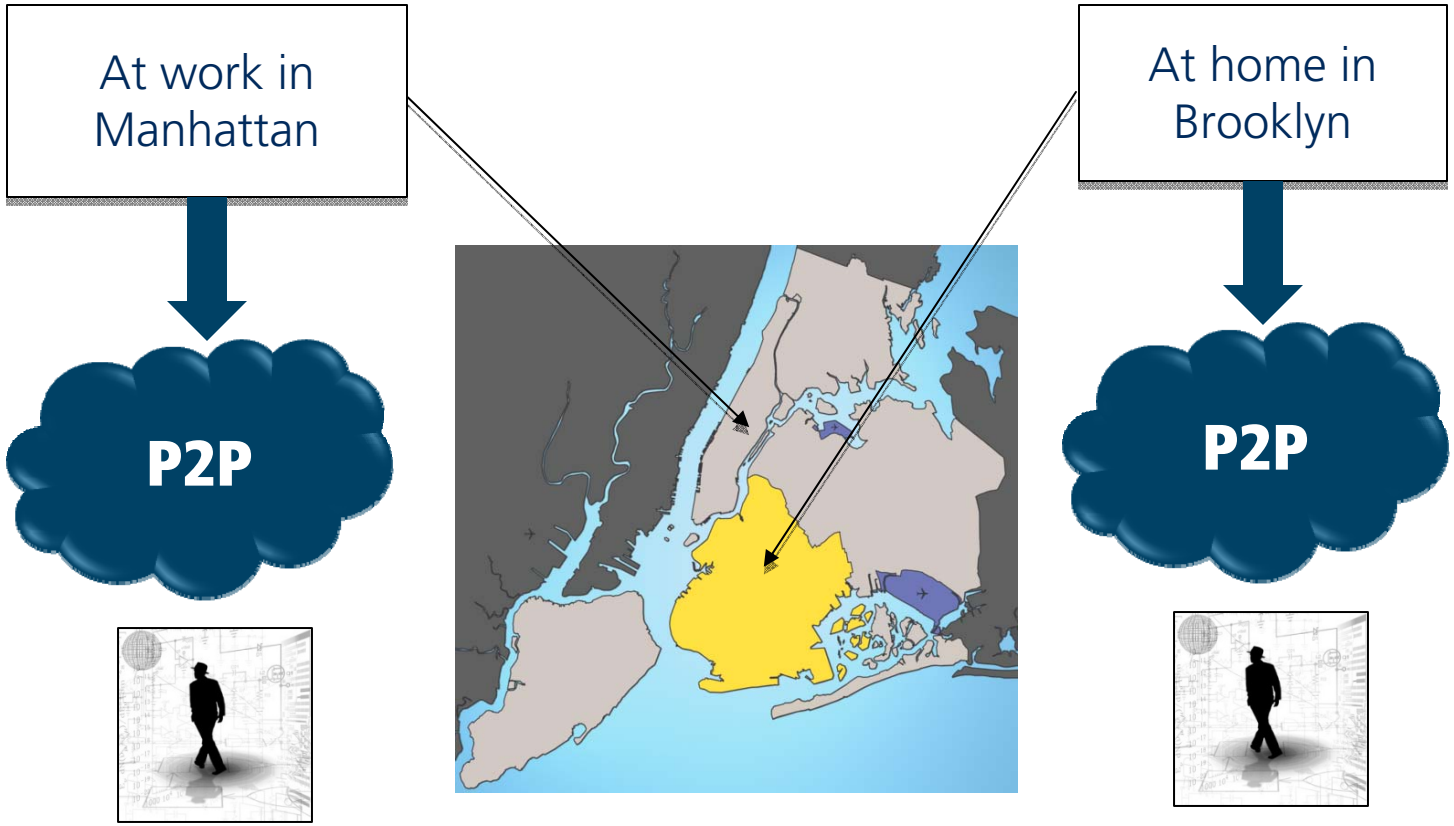
Vendor Case Example: Security Software Firm





1. Highly technical project files located on P2P
2. Source was determined to be vendor, not bank
3. Detailed forensic report indicating IP, person's name, other files, geographic location, ISP
4. Multinational confronted vendor with evidence
5. Vendor found its project leader had P2P software running on portable machine
6. Project leader disclosed this and four other bank's sensitive project details
7. Files found in possession of information concentrator in Brazil
8. Project delayed an reworked

Internal case example: board minutes



1. Executive Assistant to C level executive released highly branded, large financial services company board minutes, compliance audit results, and financial plans
2. Firm found out because private-eye found board of directors personal cell phone and called members over vacation weekend
3. Files located and quickly removed – spread unclear

Hospital Disclosure Case

2 Spreadsheets contained this information for each record…

1. FAFA billNumber
2. providerName
3. providerAddressLine1
4. providerCityStateZip
5. providerPhoneNumber
6. providerFederalTaxId
7. patientFirstName
8. patientMiddleInitial
9. patientLastName
10. patientSSN
11. patientPhone
12. patientAddressLine1
13. patientAddressLine2
14. patientCity
15. patientState
16. patientZipCode
17. patientSex
18. patientBirthDate
19. patientEmployerName
20. patientEmployerAddressLine1
21. patientEmployerAddressLine2
22. patientEmployerCity
23. patientEmployerState
24. patientEmployerZipCode
25. patientEmployerPhone
26. caseType
27. admissionDate
28. dischargeDate
29. patientMedRecNo
30. patientMaritalStatus
31. guarantorFirstName
32. guarantorLastName
33. guarantorSSN
34. guarantorPhone
35. guarantorAddressLine1
36. guarantorAddressLine2
37. guarantorCity
38. guarantorState
39. guarantorZipCode
40. guarantorBirthDate
41. guarantorEmployerName
42. guarantorEmployerAddressLine1
43. guarantorEmployerAddressLine2
44. guarantorEmployerCity
45. guarantorEmployerState
46. guarantorEmployerZipCode
47. guarantorEmployerPhone
48. guarantorRelationship
49. totalCharges
50. amountBalance
51. totalPayments
52. totalAdjustments
53. accidentCode
54. accidentDate
55. firstInsuranceName
56. firstInsuranceAddressLine1
57. firstInsuranceCity
58. firstInsuranceState
59. firstInsuranceZipCode
60. firstPolicyNumber
61. firstAuthorizationNumber
62. firstGroupName
63. firstGroupNumber
64. firstInsuredRelationship
65. firstDateEligible
66. firstDateThru
67. secondInsuranceName
68. secondInsuranceAddressLine1
69. secondInsuranceCity
70. secondInsuranceState
71. secondInsuranceZipCode
72. secondPolicyNumber
73. secondGroupName
74. secondGroupNumber
75. secondInsuredRelationship
76. secondDateEligible
77. secondDateThru
78. **primaryDiagnosisCode**
79. attendingPhysician
80. attendingPhysicianUPIN
81. lastPaymentDate
82. providerShortName

…and there were *20,245 unique records*

File Titles: [redacted]

IP Location: [redacted]

IP Registration: [redacted]

Geographic Location:
[redacted]

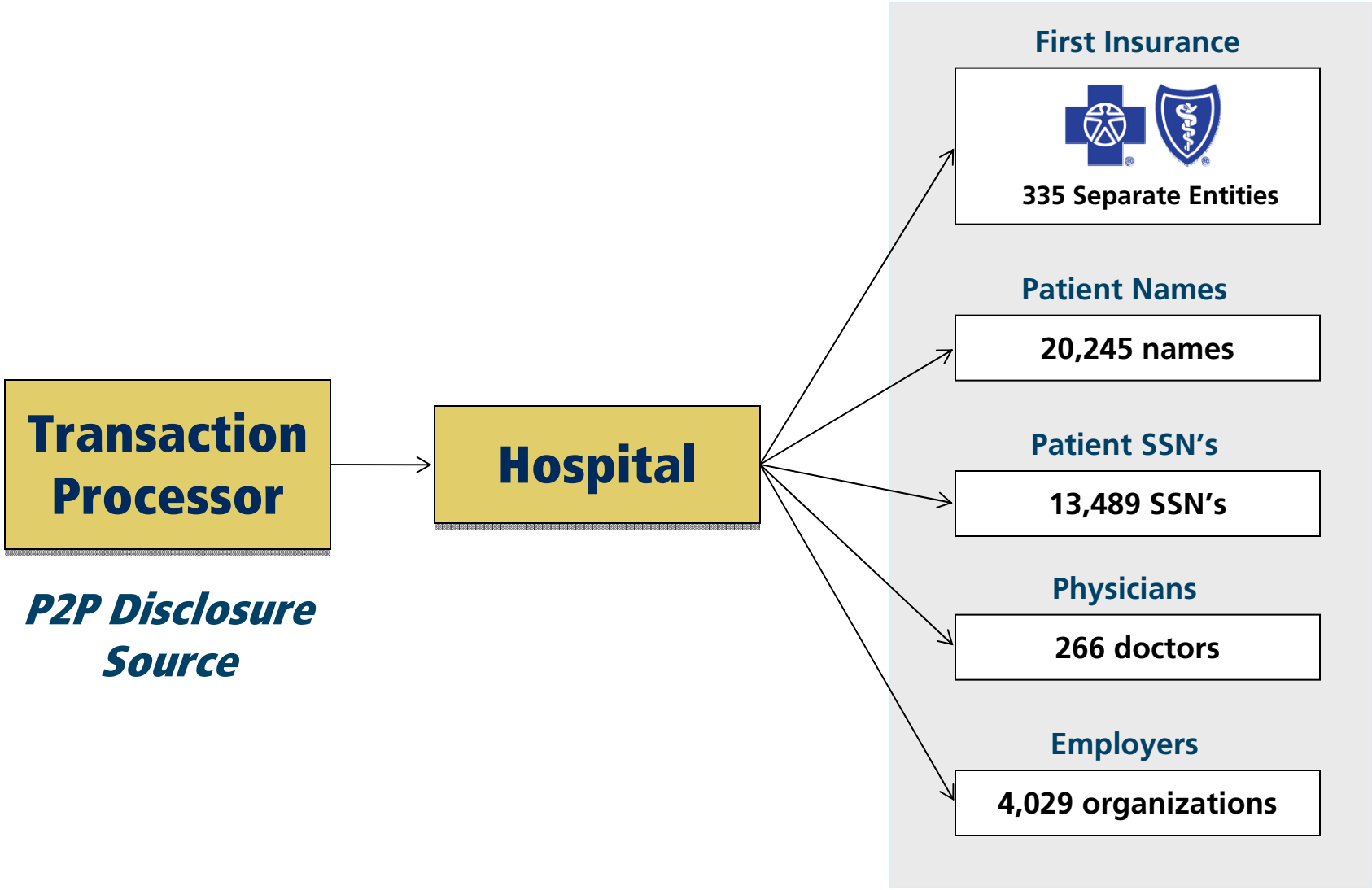
Date / Time Captured
March 11, 2008 / [redacted]

P2P Client Used
LimeWire 4.11

Disclosing Company
[redacted]

Name of Discloser
[redacted]

Extended Enterprise Impact of one data release



Agenda

- The Problem
- **Solutions**
- Questions

What do most enterprises do today?

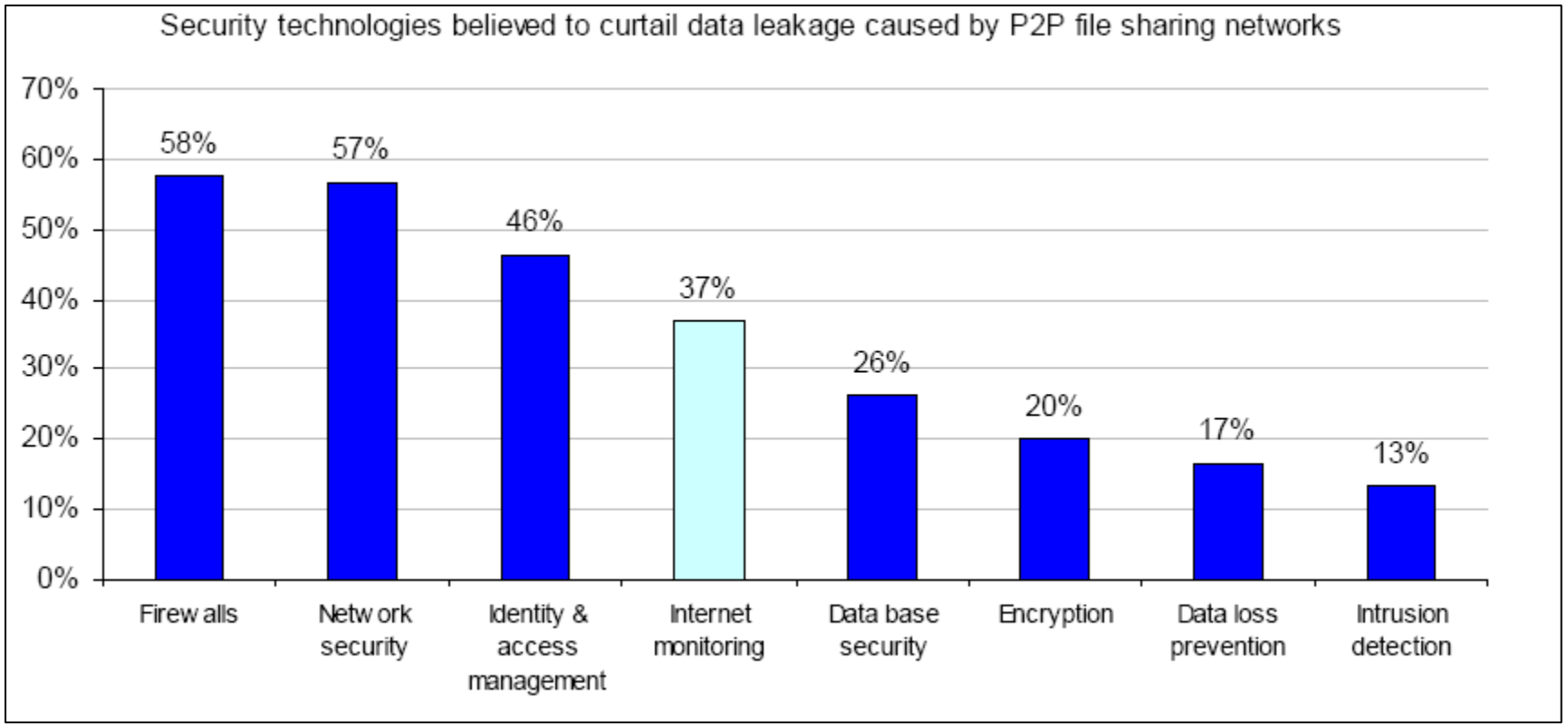
1. Policies that prohibit P2P	▪ Employees, suppliers, agents, and customers do not follow
2. Use port-scanning hardware	▪ P2P goes over web traffic (port 80)
3. Use a Firewall	▪ P2P designed to thwart firewalls (push requests)
4. Encrypt Information	▪ Users give access when using P2P
5. Lock-down computers	▪ Users go down path of least resistance – home PC's, etc.

How control information outside your perimeter?

Judge policy effectiveness?

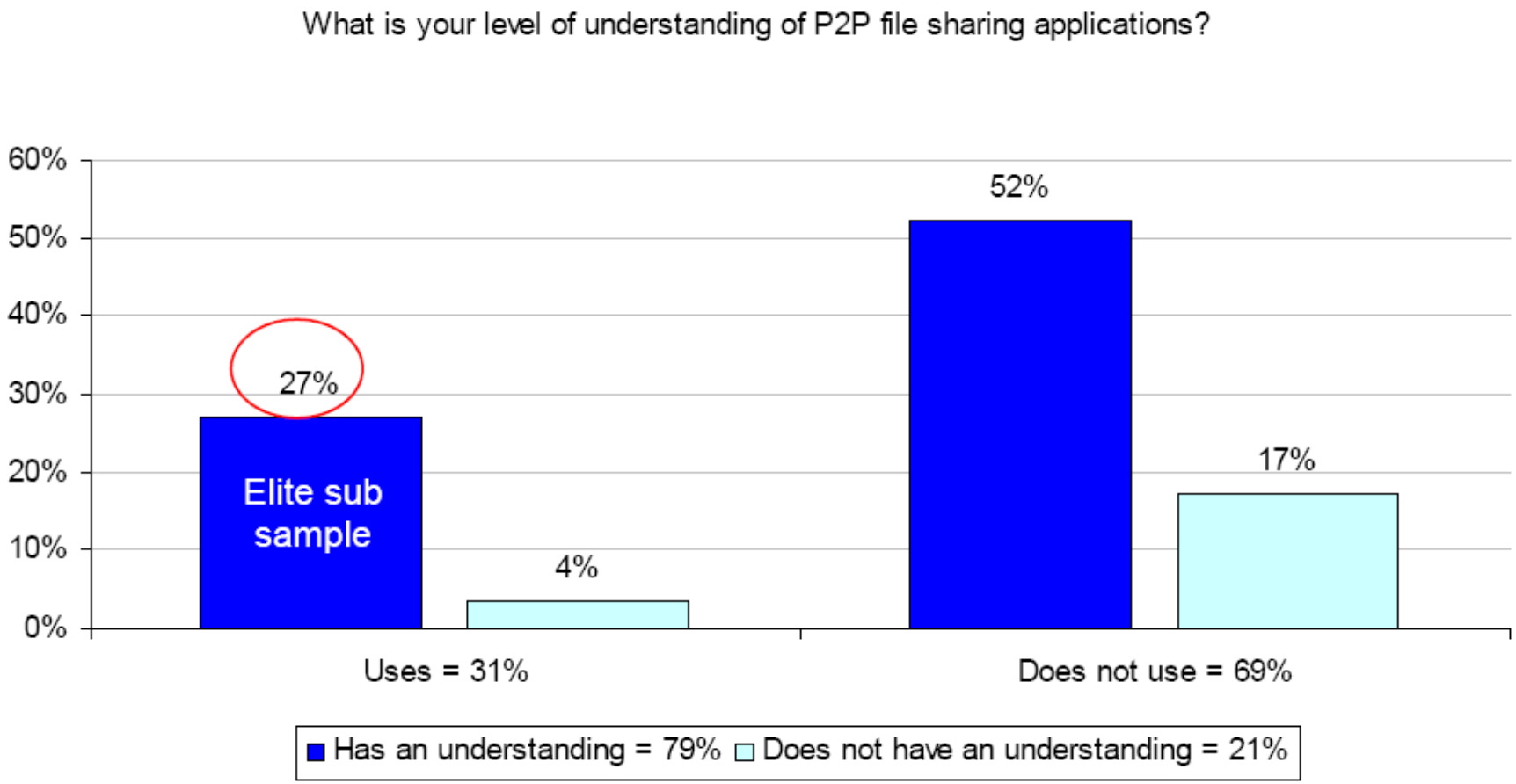
Guard against human error?

The majority of technologies believed to curtail data leakage via P2P networks is not fully effective



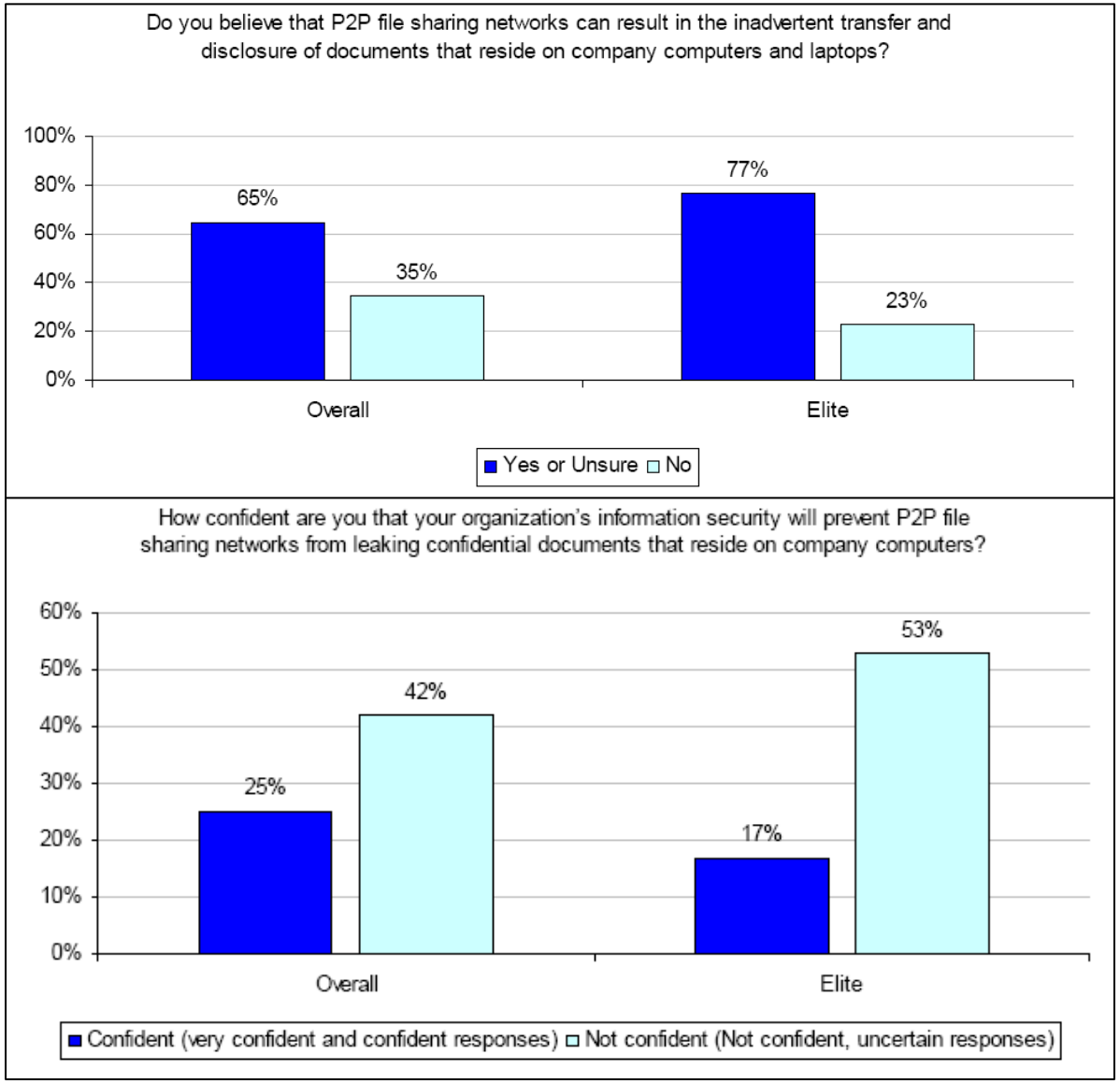
Source: Ponemon Institute – Ignored Crisis in Data Security: P2P File Sharing

It is critical to have *used* P2P file sharing application to understand all the risks



Source: Ponemon Institute – Ignored Crisis in Data Security: P2P File Sharing

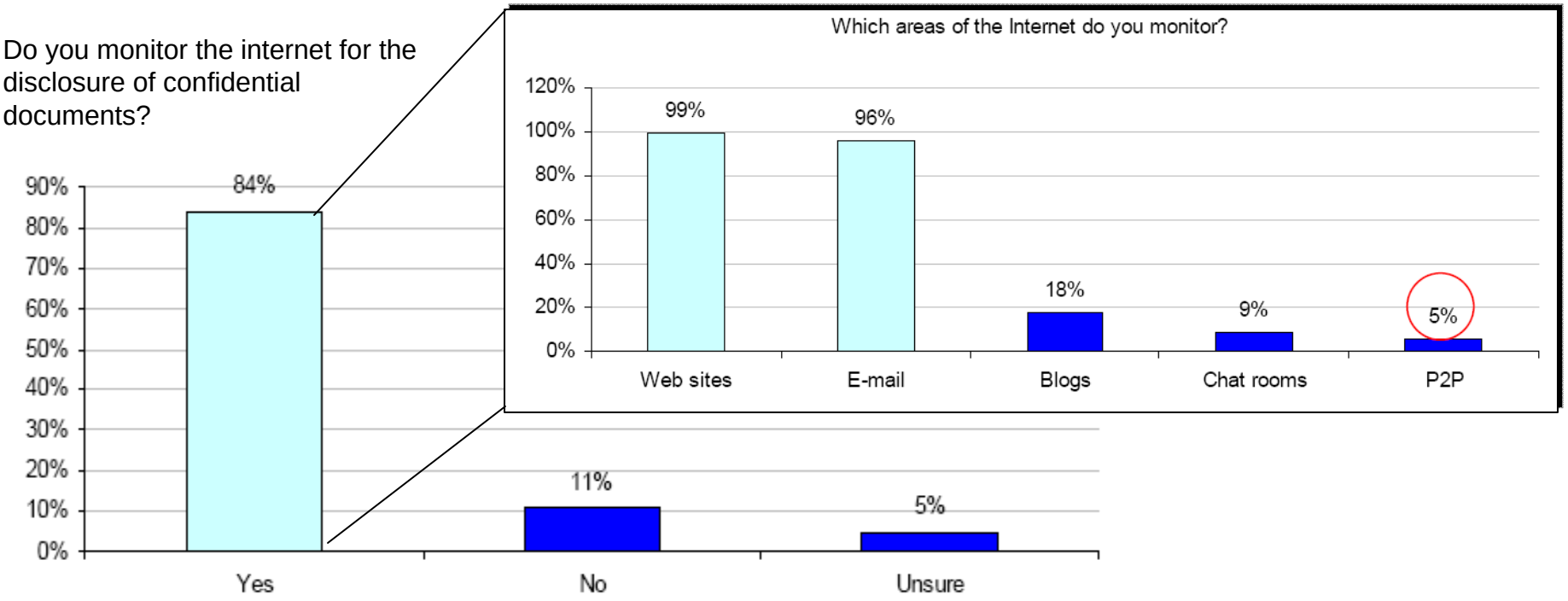
Acknowledged threat – perceived gap in prevention



Source: Ponemon Institute – Ignored Crisis in Data Security: P2P File Sharing

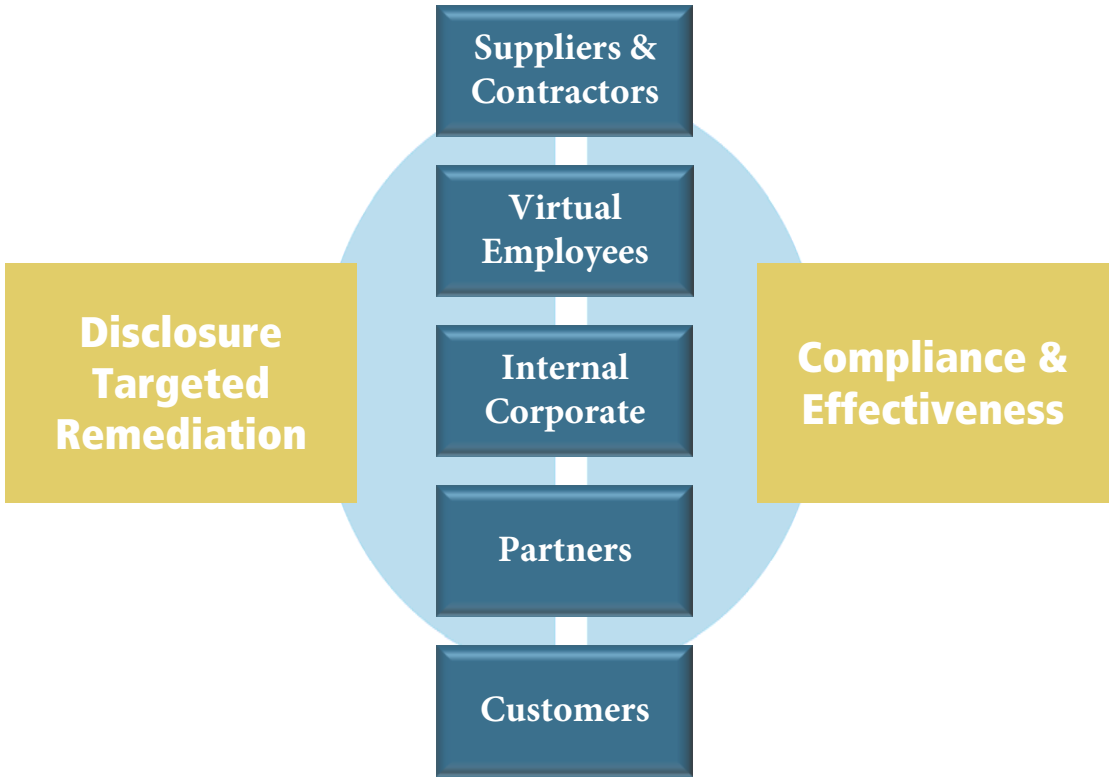
Despite recognizing a threat, very few monitor P2P file sharing networks for confidential documents

Do you monitor the internet for the disclosure of confidential documents?



Source: Ponemon Institute – Ignored Crisis in Data Security: P2P File Sharing

What you can do depends on disclosure source…



What can you do?

	Educate	Control	Identify & Measure
Internal / Employee	▪ Companywide notices, newsletters and policy emphasis ▪ Focus on high risk employees (resumes on P2P)	▪ Ensure P2P signatures identified on internal systems ▪ Expand "perimeter" to employee portable / home systems	▪ Quickly ID disclosures & evaluate control effectiveness using internal systems and external P2P monitoring
Suppliers Contractors	▪ Notify & educate offending suppliers, vendors ▪ Arm supply management group	▪ Include prohibition on P2P use as part of contracts / MSAs ▪ Demand cost reductions from high risk/repeat offenders	▪ Monitor P2P space for new disclosures ▪ Monitor P2P space for supplier / vendor compliance
Customers	▪ Establish P2P educational extranet, include advice in periodic newsletters ▪ Notify disclosing customers / arm CSRs	▪ Elevate fraud identification vigilance for exposed individuals ▪ Work with law enforcement to stop criminal use	▪ Quickly ID compromised account data via P2P monitoring

What if you knew…

- …that sensitive and confidential documents regarding your organization were publicly available on the internet?

They are…

- …that the source of these documents were not only your employees, but your vendors, partners, and even customers?

All of the above…

- …that internet users are actively searching for these documents by name?

Constantly….

- …that criminals, the media, competitors, and foreign governments use these documents and profit from them?

They do….

…what would you or could you do?

Thank You!

Chris Gormley

Chief Operating Officer

Tiversa, Inc

cgormley@tiversa.com

(724) 940-9030

.