

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009



Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or “P2P”, networks.

As P2P file-sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer-to-peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer-to-peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie

and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer’s hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

“**User error**” scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

“**Access control**” occurs most commonly when a child downloads a P2P software program on his/her parents computer. This may occur with or without the parents’ knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

“**Intentional software developer deception**” occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

“**Malicious code dissemination**” occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code (“worms”) in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user’s computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the

dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

“By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.”

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the “Inadvertent Sharing via P2P Networks,” during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previ-

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the “Google of P2P.”

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 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

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term “tax return” is also highly sought after on P2P networks. During a live demonstration in January for NBC’s Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their

tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers (“SSN”). According to a report on the black market, SSNs are worth approximately \$35. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual’s tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS’s system as “already filed.” Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn’t match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

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 abuse records
medical abuse
medical abuse records
medical algorithms
medical authorization
medical authorization form
medical authorization
medical benefits
medical benefits plan chart
medical billing
medical billing
medical bill
medical biller resume
medical billing software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

Examples to follow on subsequent pages...

	A	B	C	D	E	F	G	H	I	J	K
	providerName	patientFirstName	patientLastName	patientSSN	patientPhone	patientAddressLine1	patientCity	patientZipCode	patientSex	patientBirthDate	primaryDiagnosisCode
93311	HOSPITAL	SAMUELA					HOUSTON	77033	Female	12/4/1978	522.31
93312	HOSPITAL	MONIQUE					BRIDGE CITY	77611	Female	1/23/1971	784
93313	HOSPITAL	PAMELA					BRIDGE CITY	77611	Female	2/26/1961	786.5
93314	HOSPITAL	MATHEW					BRIDGE CITY	77611-0000	Male	4/18/1992	873.44
93315	HOSPITAL	JAMIE					HIGH ISLAND	77623	Male	3/21/938	786.5
93316	HOSPITAL	WILLIAM					DALLAS	75216	Male	11/7/1933	V58.3
93317	HOSPITAL	ANDREA					PORT ARTHUR	77642	Female	12/10/1970	278.81
93318	HOSPITAL	BRENT					WIDOR	77992	Male	4/25/1977	780.5
93319	HOSPITAL	ESPERANZA					GRAND PRAIRIE	75052	Female	7/14/1945	785.83
93320	HOSPITAL	BRIAN					DALLAS	75216	Male	5/18/1975	789
93321	HOSPITAL	JAMIE					PORT NECHES	77651	Male	12/22/1917	V70.0
93322	HOSPITAL	JOHNNY					HOUSTON	77022	Male	1/26/1969	451.21
93323	HOSPITAL	JOHNNY					DALLAS	75211	Male	12/4/1961	786.57
93324	HOSPITAL	GARY					BRIDGE CITY	77611	Male	11/11/1956	611.71
93325	HOSPITAL	STEVEN					GRANGE	77632	Male	11/24/1966	6.8
93326	HOSPITAL	CARMEN					DALLAS	75224	Female	1/26/1961	786.5
93327	HOSPITAL	GREGORY					PT ARTHUR	77642	Male	7/20/1976	553.1
93328	HOSPITAL	DAVID					RICSBOTD	75115	Male	10/14/1954	724.2
93329	HOSPITAL	SHANA					GRANGE	77630	Female	8/9/1979	719.45
93330	HOSPITAL	MICHAEL					PORT ARTHUR	77642	Male	1/9/1970	278.81
93331	HOSPITAL	RUDOLPH					BRIDGE CITY	77611	Male	3/21/1956	786.73
93332	HOSPITAL	YOLANDA					DALLAS	75237	Female	1/12/1970	V72.83
93333	HOSPITAL	JOE					DALLAS	75224	Male	2/7/1967	414.81
93334	HOSPITAL	ROSIE					DALLAS	75233	Female	12/25/1994	822.7
93335	HOSPITAL	SYLVIA					HOUSTON	77019	Female	2/4/2000	780.5
93336	HOSPITAL	KENNETH					CHAR HILL	75134	Male	5/21/1969	521
93337	HOSPITAL	ELVIRA					PORT ARTHUR	77642	Female	5/23/1999	787.83
93338	HOSPITAL	HENRY					HOUSTON	77039	Male	7/27/1993	719.41
93339	HOSPITAL	MERCEDES					DALLAS	75224	Female	8/21/2002	343
93340	HOSPITAL	JERRY					PORT ARTHUR	77642	Male	1/31/1952	724.2
93341	HOSPITAL	CAROL					PORT ARTHUR	77642	Female	11/17/1941	822
93342	HOSPITAL	A					GRANGE	77632	Male	3/8/1936	429
93343	HOSPITAL	CALEB					PORT ARTHUR	77642	Male	2/10/2000	787.83
93344	HOSPITAL	JOSIE					DALLAS	75211	Male	1/11/1967	882.2
93345	HOSPITAL	MARY					DALLAS	75224	Female	1/29/1927	664.9
93346	HOSPITAL	L					DALLAS	75211	Male	4/24/1933	786.3
93347	HOSPITAL	BRIAN					DALLAS	75216	Male	5/18/1975	564
93348	HOSPITAL	PATRICIA					PORT ARTHUR	77642	Female	11/4/1952	725.5
93349	HOSPITAL	MARVA					HOUSTON	77039	Female	4/30/1961	666.12
93350	HOSPITAL	EMERQUE					HOUSTON	77033	Male	1/23/1959	279.27
93351	HOSPITAL	EMERALDA					DALLAS	75211	Female	3/14/1986	564
93352	HOSPITAL	DANIELA					PORT ARTHUR	77642	Female	2/11/2003	287.83
93353	HOSPITAL	ALESSANDRA					HOUSTON	77037	Female	3/31/1969	786.1
93354	HOSPITAL	JOHN					SABINE PASS	77855	Male	2/11/1963	525.3
93355	HOSPITAL	CARLOS					HOUSTON	77031	Male	4/23/1979	276.11
93356	HOSPITAL	JOYCE					DALLAS	75211	Female	8/17/1933	422.1

	A	B	C	D	E	F	G	H
	Last	First	SSN	Taxable?	Degree	School	Major	Division
1000		John		N	Certificate	CFA Institute	CFA	Eastern
1001		Zishan		N	Graduate	NYIT	MBA	Western
1002		David		N	Certificate	CFA Institute	CFA	Western
1003		Anthony		N	Graduate	Stevens Institute	MIS	Eastern
1004		Melissa		N	Certificate	Dowling College	CFP	Eastern
1005		Thomas		N	Certificate	Pace	CFP	Eastern
1006		Mary Linley		N	Certificate	American College	CFP	Eastern
1007		Samuel		N	Certificate	Kaplan University	CFP	Eastern
1008		Sandeep		N	Graduate	Steven Institute	Info Mgmt sys	Eastern
1009		Emmee		N	Certificate	Kaplan	CFP	SouthWest
1010		Scott		N	Certificate	Kaplan	CFP	Western
1011		Darya		N	Undergrad	Montclair State University	Marketing	Eastern
1012		Isaac		N	Certificate	Pace University	CFP	Eastern
1013		Sotland		N	Certificate	Kaplan	CFP	Eastern
1014		James		N	Certificate	Kaplan	CFP	Eastern
1015		Steven		N	Graduate	University of Connecticut	MBA	Eastern
1016		Michael		N	Graduate	Stevens Ins	MIS	Eastern
1017		Alejandra		N	Degree	Pace University	BA	Eastern
1018		Hasan		N	Undergrad	NYU	International MBA	Eastern
1019		Sneh		N	Undergrad	Stevens Institute	MIS	Eastern
1020		Luis		N	Undergrad	Axia College	BA	Eastern
1021		Jared		N	Certificate	Kaplan	CFP	Eastern
1022		Matthew		N	Undergrad	Brooklyn College	Finance	Eastern
1023		Francisco		N	Certificate	CFA Institute	CFA	Eastern
1024		Belinda		N	Undergrad	Universidad	Accounting	PR

Ssn/Sin: [] Employer: [] Local: 952 Status: 03 Paid Thru: Jul/1987
 Name: WANDA Gender: F BirthDate: 09/21/1942
 Address: [] CA
 Phone: [] Sjc: [] VoterReg: No BA: 085 Mail: []
 Initiation: 01/13/1977 Seniority: 08/01/1980 CkoAuth: [] Salary: \$13.00
 Reinitiation: [] Rehire: [] TermLcl: [] TermEmp: 01/15/1987
 DuesRate: \$26.00 NormAmt: \$26.00 DuesDvg: [] DuesLast: 06/15/1987
 InitRate: \$100.00 InitPd: \$100.00 Start: [] Dept: []
 FeniRate: \$0.00 FeniPd: \$0.00 Original: Oct/1977 Clock: []
 Beneficiary: [] Relation: 3 Koj: 010 TransRate: \$0.00
 TransferTo: [] From: [] Koj2: [] TransPaid: \$0.00
 Remarks: TERM 1-87*****WATCH****
 Asses 1: [0] 2: [0] 3: [0] 4: [0] PostFlag: [] PostDate: []
 Party: [] Precinct: [] **PAYMENTS**
 Record: [] 69495 [] of 69495

Insurance Aging

INCORPORATED

JOHN J [] Date of Birth: 0/28/1945 Insured: Self

Insurance: Primary ID: []

Billing	Date	Code/CPT	Billed	Amount	Current	31-80	81-90	91-120	> 120	Total
			05/01/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			12/17/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			04/30/2007	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Patient Total:				220.00	0.00	0.00	0.00	0.00	220.00	220.00
Insurance Total:				379.16	0.00	0.00	0.00	147.76	231.40	379.16

TIMOTHY L [] Date of Birth: 02/21/1945 Insured: Self

Insurance: Primary Group Number: 00001022 ID: []

Billing	Date	Code/CPT	Billed	Amount	Current	31-80	81-90	91-120	> 120	Total
210464	02/17/2008	87086/87086	03/08/2008	41.00	0.00	0.00	0.00	0.00	41.00	41.00
			08/10/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
			12/08/2006	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Patient Total:				41.00	0.00	0.00	0.00	0.00	41.00	41.00

DANNY T [] Date of Birth: 01/15/1948 Insured: Self

Insurance: Primary Group Number: 00000905 ID: []

Billing	Date	Code/CPT	Billed	Amount	Current	31-80	81-90	91-120	> 120	Total
233355	05/19/2008	87086/87086	08/09/2008	41.00	0.00	0.00	0.00	0.00	41.00	41.00
Patient Total:				41.00	0.00	0.00	0.00	0.00	41.00	41.00
Insurance Total:				82.00	0.00	0.00	0.00	0.00	82.00	82.00

BEN [] Date of Birth: 11/28/1935 Insured: Self

Insurance: Secondary ID: []

Billing	Date	Code/CPT	Billed	Amount	Current	31-80	81-90	91-120	> 120	Total
---------	------	----------	--------	--------	---------	-------	-------	--------	-------	-------

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25-4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and

protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.



144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com