Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Identity Theft

The act of identity theft can be performed by anyone, it could be family, friends or spouses. The internet provides a faceless median by which even a fourteen year old can partake in this criminal activity. This is the very reason companies are beginning to educate the population on personal information safety and what to do in the event of data theft.

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Identity Theft

GSEC Gold Certification

Author: Ian Wolff, iwolff@du.edu

Adviser: Jim Purcell

Accepted:

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Outline

1. Introduction
2. Analysis of Major Issues
    a. Security Awareness across the Generations
    b. Increased E-Commerce Data use Protection
    c. What is the Government Doing to Help?
    d. Corporate Responsibility of Data Protection
    e. What do you do after fraud is committed?
3. Conclusions
    a. Security Awareness across the Generations
    b. Where is the Government in this fight?
    c. Are businesses taking appropriate actions?
    d. Is technology our friend or foe?
4. Final Thoughts on Identity Theft
5. References

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

The Information Age is upon the world and new types of crimes are being carried out on a daily basis. The internet provides the world with immediate access to business and personal data. Additionally, it allows us to take part in a multitude of activities that affect other people's lives. September 11th, 2001 marked a coming of age for security initiatives, physical and data alike. Physical security issues are fairly easy to address, the main focus becomes data security and will have to be taken more seriously in the future. Cyber crimes can range from holding a network hostage with Denial of Service attacks or simply stealing data from a company's databases. One of the most damaging of cyber crimes is identity theft. John Vacca defines identity theft in a manner in which we can all understand, "Quite simply, identity theft is the appropriation of an individual's personal information to impersonate that person in a legal sense" (Vacca, pg 4).

The concept of identity theft is nothing new, it has been around for centuries in one form or another. According to the Identity Theft Resource Center (ITRC), a non-profit organization dedicated to helping victims of identity theft, seven million people fell victim to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

identity theft within the last twelve months[1]. This may not seem like much especially since our population goes into the hundreds of millions, but one must consider the time and money it takes to recover.

The act of identity theft can be performed by anyone, it could be family, friends or spouses. The internet provides a faceless median by which even a fourteen year old can partake in this criminal activity. This is the very reason companies are beginning to educate the population on personal information safety and what to do in the event of data theft.

Identity theft crimes that occur are being recognized quicker, and the recovery time is taking longer. Data shows that the time to recover has risen from 175 hours to 600. Due to the faceless component, convicting thieves is becoming harder and harder and the paper trail is almost imperative (Mendell, pg 218).

Thomas Mendell, categorizes identity theft into two categories. These categories include personal and business (Mendell, pg 219). Mendell does go into the different techniques used by criminals who partake in identity theft activities. These are[2]:

- Stealing
- Research
- Observing data
- Deceiving others
- Cracking into computer systems
- Locating the information or documents
- Soliciting under false pretenses
- Retrieving the information or documentation

[1] http://www.idtheftcenter.org/facts.shtml
[2] The bullet points above were taken from "Investigating Computer Crime in the 21st Century" page 219

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

As observed from the above bullets, the process of stealing data is no different than any other elaborate criminal scheme. The only thing that changes is the medium by which the data is obtained.

The government has taken a stance to help place responsibility back on those who deserve it. The downside of course is that this is moving at a slow pace and is on hold due to the current global situation. Businesses will not take the front line on this fight until their hand is forced by legislation. While it would be nice to think that consumers would lead the fight, businesses do well to ignore their concerns. According to the Silver Lake Editors, 40% of all consumer complaints in the United States are that of identity theft. They also go on to say that the damage from this crime costs 1.4 billion dollars in 2004 and project that it will cost 3.6 billion dollars in 2006 (Silver Lake, pg. 1-2).

The future of technology will be controlled by such things like biometrics, smart cards, optical cards, or for the more hardcore a national ID card. These are some of the ways that have been discussed and implemented by security experts to help consumers and businesses protect themselves from identity theft. However, even with all advanced technology there are flaws in the design as well as arguments against their use. The question will become, can these technologies be properly developed and integrated into every day consumer lives?

There are a great deal of issues that need to be addressed when the topic of identity theft is broached. A wide range of measures can be taken by businesses, consumers and the government that could help curb the epidemic that we are faced with. The ever expanding

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

selection of technologies being developed is taking the average population longer to catch up. The following research shows that with the help of technology, legislation and general consumer awareness identity thieves can be thwarted.

© SANS Institute 2007, Author retains full rights.

Identification of Major Issues

- Educating the general population worldwide on Identity Theft awareness.
- Government regulations and legislation must be passed to force companies to better protect customer data.
- Increasing technology capabilities to better track and thwart identity theft criminals.
- Can a regulating body be put together to help create a global effort to stop identity theft crimes?
- Increasing E-Commerce use and unprotected data transfers.
- The two sided story of data mining and data protection best practices.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- Corporate policy creation to avoid responsibility of data protection to certain degrees.

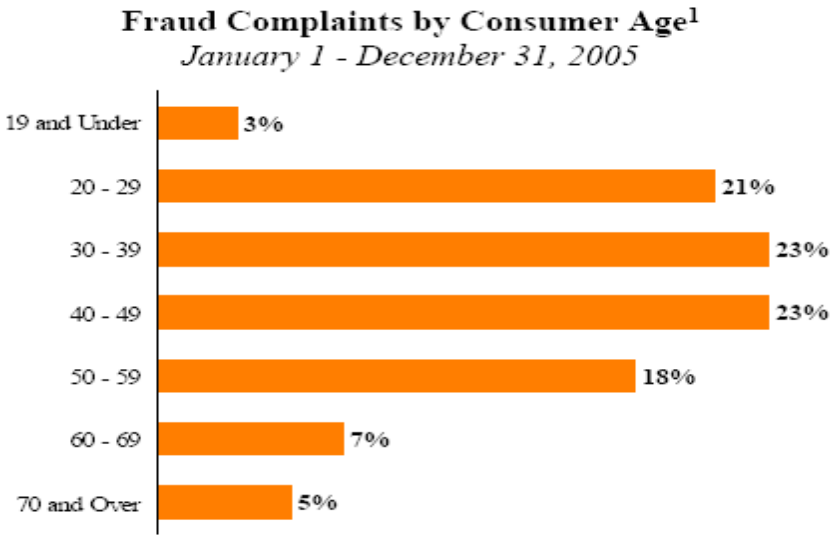
© SANS Institute 2007, Author retains full rights.

2. Analysis of Major Issues

Security Awareness across the Generations

According to Consumer Sentinel, a government agency that works in conjunction with the Federal Trade Commission, any age set is subject to identity theft.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.



[3]

The graph shows a majority of cases come from 20 to 59 which essentially is a majority of the population. The question here becomes, where does the responsibility lie in terms of user education and awareness? It's obvious by these statistics there is no specific age gap that is more susceptible to falling victim. One fact is apparent, identity theft is a negative product of sharing data across electronic mediums, similar to spam and phishing (Silver Lake, 173).

Who is primarily responsible?

The easy answer to identity theft awareness and prevention must first fall on the consumer themselves (Silver Lake, pg 173). The Silver Lake Editors, authors of *Identity Theft: Protect Your Name, Credit and Information*, make very good points concerning relying on the authorities to educate consumers. There are too many transactions and data being passed for every corporation or authoritative body to go out and ensure everyone has the proper training and is being watched. Another reason each consumer must be

[3] The graph used above was used from Consumer Senitenal: http://www.consumer.gov/sentinel/Sentinel%20CY-2005/fraud_complaintsbyage.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

primarily responsible is because of who is ultimately affected by identity theft; the consumer themselves. The consumer must spend the money, which can be up to $1,600 dollars of personal funds[4], and that does not include post mortem such as credit issues and in some cases loss of employment.

Thomas Mendell breaks down the different categories of data that can be stolen. There are three types; physical, operational, and information based (Mendell, pg 221). Physical ways to obtain sensitive data is by identification cards. This can occur by sifting through mailboxes and garbage as well as consumers losing identification cards. Operational examples include not shredding papers, shoulder surfing and retail transactions. Finally, the last category is information based which includes social engineering, unsecured websites and just plain searches through search sites such as Google (Mendell, 221).

What are some steps that can be taken to protect yourself?

What are some preventive measures that can be taken to help protect against identity theft? Listed below are just a few that are suggested by consumer watchdogs[5]:

- Do not carry individual Social Security Cards.
- Limit who you give sensitive information to over the phone, e.g. bank account numbers, social security numbers, etc.
- Shred all documentation that may contain personally identifiable numbers, e.g. credit card applications, receipts, etc.
- Keep a close on utility bills and credit card bills to ensure that the charges being made are in fact yours.

[4] http://www.idtheftcenter.org/facts.shtml: Fact number 7
[5] Tips were provided by Silver Lake Editors on page 180 under the "Prevention: Quick Tips" section

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The list above gives physical tips to safeguarding information, but what are some internet type tips that could help. The following addresses some of these concerns:

- Using different passwords for each account that is accessed online.
- Use complicated passwords that have seven or more characters and use special characters such as @ !.
- Do not write passwords down on anything that is visible to the general public.

Increased E-Commerce Data use Protection

What is Internet Identity Theft?

This question may seem overly obvious to most, but there is a major difference between having something physical stolen and having something stolen on the internet. The primary difference is the ability to track who, when and how the theft occurred. Below is a graph from Consumer Sentinel to help get a feel for the numbers seen regarding online identity theft.

As shown in the graph below, the number of total complaints reported are approximately half when compared with the total number of complaints with amounts paid.

Total Number of Fraud Complaints & Amount Paid

Calendar Years 2003 through 2005

CY	Total No. of Complaints	Complaints Reporting Amount Paid	Percentage of Complaints Reporting Amount Paid	Amount Paid Reported	Average Amount Paid[1]	Median Amount Paid[2]
2003	327,479	254,151	78%	$459,570,221	$1,808	$222
2004	406,193	307,681	76%	$567,881,779	$1,846	$263
2005	431,118	282,874	66%	$682,348,612	$2,412	$350

[6]

Different Types of Identity Theft Methods

[6] Courtesy of Consumer Sentinel http://www.consumer.gov/sentinel/Sentinel%20CY-2005/totalfraudcomplaints_amountpaid.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

John Vacca, author of *Identity Theft* describes the different types of activities that can be associated with different internet criminal activities. This is a good way to help discern the differences between physical and internet identity thefts. The graphic below helps illustrate that while only about two percent of reported fraud is internet email, the cost of recovery is still incredibly high.

Other Identity Theft

Theft Subtype	Percentages CY-2003	Percentages CY-2004	Percentages CY-2005
Evasion of Legal Sanctions	2.1%	2.4%	2.2%
Internet / E-mail	1.6%	1.8%	1.9%
Medical	1.8%	1.8%	1.8%
Apartment / House Rented	0.9%	0.9%	0.9%
Insurance	0.3%	0.4%	0.4%
Property Rental Fraud	0.2%	0.3%	0.3%
Bankruptcy	0.3%	0.3%	0.3%
Child Support	0.2%	0.3%	0.2%
Magazines	0.1%	0.2%	0.2%
Securities / Other Investments	0.2%	0.1%	0.2%
Other	11.6%	14.4%	17.6%
Total	**19%**	**22%**	**25%**

[7]

New Account Creation

The first and easiest is new account creation which simply consists of using personal information to open accounts for credit cards. All the information needed in most cases is information easily found through public access methods, such as Googling specific personal information (Vacca, pg 66).

Bank Fraud[2]

Theft Subtype	Percentages CY-2003	Percentages CY-2004	Percentages CY-2005
Electronic Fund Transfer	4.8%	6.6%	7.9%
Existing Accounts	8.3%	8.5%	7.4%
New Accounts	3.8%	3.6%	3.3%
Unspecified	0.5%	0.1%	0.1%
Total	**17%**	**18%**	**17%**

[8]

Account Takeover

[7] Graphic taken from http://www.consumer.gov/sentinel/Sentinel%20CY-2005/victim_info_misused.pdf
[8] Graphic taken from http://www.consumer.gov/sentinel/Sentinel%20CY-2005/victim_info_misused.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

This form of identity theft takes place in several different ways. Each way is linked to tricking an individual into giving up their personal information. The information obtained is then used to login to existing accounts and where the "thief" then can make purchases. Another way to obtain personally identifiable data is through cloning a site. This means that a site is made to look like a business site and while the consumer orders a product all information is actually going to the criminal (Vacca, 66-67). This is most popularly referred to as phishing, but can occur through redirection of URL links.

Fraudulent Transactions

This is the most common type of identity theft method because it is the quickest and easiest way for criminals to get around. This virtually anonymous "robbery" causes the most damage in the least amount of time while keeping the criminals identity hidden (Vacca, 67-68).

What is the Government Doing to Help?

The country has seen identity theft issues for decades and this prompted the government to put many different types of legislation in place. There is not only legislation at the federal level, but also at the state level. Interestingly enough a good deal of the legislation put in place are ten to twenty years old and only vaguely address online data theft. It was not until 1998 that a bill was actually passed, Identity Theft and Assumption Deterrence Act, at the federal level that finally defined identity theft as a federal crime (Silver Lake, pg 127).

Identity Theft and Assumption Deterrence Act

Until this Act was put into place identity theft victims were not seen as victims, instead they were forced to fight the battles themselves. This in the end affected

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

how quick the recovery was or even if there was recovery, but with this Act in place the following happened[9]:

- Helped identify people who had their credit compromised and money stolen as true victims. The victims could include the business that lost their information as well.
- Defined the Federal Trade Commission (FTC) as the "central point of contact" (Silver Lake, 128) for victims to report any identity theft. This allowed for data collection and analysis of trends to find flaws in the system. It also helped law enforcement to have one central repository of data.
- It allowed the courts to hand down harsher punishment as well as seizure of assets so that the victim could get back whatever was stolen.
- Previously it was only illegal to possess or produce false identification and documents. This Act made it illegal to steal anyone else's personally identifiable information (Silver Lake, pg 128).

This Act was clearly needed to close up any discrepancies that lingered from old and out of date legislation. Fortunately, this Act led the way for other initiatives that would help with centralizing responsibilities.

ID Theft Clearinghouse

Since the FTC became the central point of contact for data theft issues, they decided to create a hotline for quicker reporting abilities. This occurred in 1999, and with this hotline creation the FTC developed the Consumer Sentinel Network. Why was this so important? The centralized database allowed for direct access by other

[9] The following bullets are summarized from points taken from the Silver Lake Publication on page 127-128.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

government agencies to analyze trends and other details directly from their offices. It only took a year of operation and the database logged over 30,000 complaints, in 2001 it logged 86,000 and in 2002 it captured nearly 200,000 (Silver Lake, 129). The downside to all of this though is that the FTC does not actually have the power to investigate or enforce any violations. This is left to federal agencies such as the Department of Justice or the Federal Bureau of Investigations.

The Sentinel Network is currently accessible by foreign bodies and international agencies. They will first, however, have to sign and agree to a confidentiality agreement that is strictly enforced and monitored[10]. This international effort combined with domestic agencies allows for the ability to crack down on organized crime through analyzing the trends. It also allows for the freeing up of resources and delegating responsibilities beyond just one agency.

The Patriot Act

The Patriot Act of 2001 is perhaps the most controversial legislations passed by the government in many years. This Act now allows federal agencies to pursue suspected identity theft criminals with more authority. Essentially, this allows officials to proceed with an investigation with only a hunch of criminal activity. The Patriot Act also forced financial institutions to do a more thorough job of verifying identities upon new account activation. This required organizations, such as banking companies, to develop procedures that would help identify and secure data in a reasonable manner (Silver Lake, pg 139-140).

[10] The confidentiality agreement can be found at http://www.ftc.gov/sentinel/confidentiality.htm

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

California Anti-ID Theft Law

The California Anti-ID Theft Law came about around the same time as the Patriot Act was announced and brought to light the issues surrounding data theft. This law allows for consumers to have more power over the information that they provide to financial institutions. Consumers have been forced to use their Social Security Numbers on everything without much say. This now enforces financial institutions to secure the Social Security Numbers in online transactions through encryption. It also put a stop to sending documents via mail with personally identifiable information on it. The most important part of this law is that any company that comes across compromised consumer data has to notify the individual. This notification is mandatory even if there is only one person affected. Most laws that are centered around this concept specifically define how many consumers have to be affected; this can be up to almost 1,000 in some cases.

California paved the way for other states to improve their data security laws and enforce harsher penalties. Although, other states have not taken it to the extent of California, it certainly improved the situation. States such as Georgia, New York and Virginia amended laws in, 2002, which helped lengthen sentences and raise fines. The by-product of all these laws led to the acknowledgment that technological advances were needed among corporations to help prevent any undesirable situations.

Standardized ID cards

One approach being taken by some government and business factions is that a standardized national identification card should be issued. The ID card would contain the obvious information, similar to a driver's

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

license, but it would also contain a smart card. Smart cards allow for a wide range of data to be stored locally on the card. Information such as bank account passwords or even biometric information can be placed on the card. The smart card idea has been embraced by many European countries as well as some Latin American countries.

Naturally, there is a wide range of opposition to this idea of standardization and arguments come from an assortment of different factions. Civil liberties groups see the use of national ID cards as a way to track an individual's personal attributes that may have nothing to do with national security. Others argue the data being kept within the smart card will be used for more marketing than actual data protection. The main concern though is the notion of what happens when the card gets stolen. If one thinks of all the data that could be stored on a smart card, especially biometric data, the possibilities become endless. This means that not only will someone have personally identifiable information, but they will have thumbprints or even retina scan features. How could anyone argue with an identity that has biometrics to back it up?

Laws that Help Criminals?

The authors of *Identity Theft: How to protect your name* make an interesting observation about the countries lack of accountability. There are some state and county laws that actually require the posting of personally identifiable information on the internet. This information can range from mortgage applications to marriage licenses, all of which contain sensitive data. Fortunately, consumers took appropriate action to help curb this. How can consumers be responsible for catching everything? Some laws put into place to help against tax fraud actually have

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the potential to compromise sensitive data. This data can be requested at anytime by a "reasonable business" that has "legitimate business purposes", all with the backing of supposed tax fraud laws (Silver Lake, pg 145).

Corporate Responsibility of Data Protection

The biggest battles at hand come from corporations' unwillingness to accept responsibility for protecting their customer data. There are plenty of reasons why this is pretty standard across the board:

- Loss of business through damaged reputation
- Closure of business if enough customers are affected
- Fines and penalties for negligence

For this reason it would be safe for someone to assume an organization should take the proper measures to avoid any possible compromise, sadly this is not the case though. Fortunately for consumers, the government has put laws into place to help put the onus back on businesses. These laws were not enacted because of identity theft specifically. It is mostly a by-product of the Enron and WorldCom scandals.

Company Data Privacy Policies

There is a breakdown even in the present times that points back to the lack of company policies and standards centered on data protection. The policies needed for proper privacy and security requirements is the very foundation upon which an Information Security presence is built. These information security policies provide guidelines employees and even customers must adhere to. The policy creation does not stop there, it also points out the flaws within the company culture and even the technology infrastructure. Information security policy benefits do not stop there, with the proper communication

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

it can show consumers that the business cares about the consumer, thus generating more business.

John Vacca does define the purpose of an information security policy role. Vacca explains that a privacy policy should accomplish three things:

- "Explain a company's information practices." (Vacca, 180)
- "Identify choices that a customer might have in how his or her data is collected, used, or shared." (Vacca, 180)
- "Establish a mechanism for receiving, investigating and resolving complaints." (Vacca, 180)

The other side of this is that while the company has established the privacy policy it is up to the consumer and employee to understand it.

The second piece to an information security policy is a security policy which specifically defines its procedures on securing sensitive data. This helps clearly define what direction the technology of the company needs to go. If the policy states that data will use encryption and biometrics then the company will need to ensure that they have the proper technology. The security policy also defines what data needs to be protected and how it will be protected. The most important piece to this policy is that it is written in such a way that a customer or employee can understand it (Vacca, 181).

Finally, an information security policy needs to state how the company will respond to a data breach. The biggest issue is what happens within the time frame following the theft, and how it is communicated. Another big factor is how much data was compromised and this is where an understanding of the different laws comes into place. Most

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

organizations will only do what they have to as it is stated by the different legislations.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was passed in 1999 to force all financial institutions to coordinate regulatory functions between governmental agencies. There are certainly good and bad things that have come with this Act, but certainly the best is uniting all under one umbrella. There are well over 200 financial regulators out there primarily because of the different types of financial institutions available. As time progresses, financial institutions are using personally identifiable information as marketing tools. This is where GLBA helps to protect consumers.

The Gramm-Leach-Bliley Act, if used properly of course, has a number of requirements that create ways to protect consumers against identity theft. For example, companies that collect personal information are required to send out notices via mail that defines how they have used and will use that information. The downside to this is that it only is required once a year. What of the other eleven months of the year? This requirement applies to any business that collects personally identifiable data, even if it is a car dealership.

Another requirement that comes from GBLA is that any institution that plans on using personal data for any use besides it's own has to notify the customer. There must also be the option to opt out of having the personal data given to the business. The easiest way for an organization to do this is to use a disclosure notice that explains intended use of the data. This disclosure form is usually signed when the customer first carries out a transaction of

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

any sort. The biggest piece of this law is that the customer is given the ability to block any disclosure of personal data for any other use besides what it was intended for. This block of information sharing is limited though to only nonpublic personal data.

E-Commerce and E-Business ID Theft Issues

The ever popular Internet is used for a great many uses, one of the most prevalent uses is E-Commerce. The Internet provides a business with the ability to allow consumers to have an easy shopping experience. This easy shopping experience works both ways, but most are unaware of the dangers that lurk in the shadows. What people should be aware of is, risks that come with E-Commerce identity theft are generated mostly through human error. These human errors include unpatched web servers, poorly written code within the online applications, or the lack of compensating controls to ensure that data is not hijacked between the consumer and the business. Below is a graphic that summarizes complaints that were reported around Internet fraud.

Total Number of Internet-Related Fraud Complaints & Amount Paid

Calendar Years 2003 through 2005

CY	Total No. of Complaints	Complaints Reporting Amount Paid	Percentage of Complaints Reporting Amount Paid	Amount Paid Reported	Average Amount Paid[1]	Median Amount Paid[2]
2003	176,754	158,534	90%	$205,550,456	$1,297	$190
2004	210,727	188,675	90%	$271,305,849	$1,438	$215
2005	196,503	160,115	81%	$336,164,255	$2,100	$345

[11]

E-Commerce is something that took off in popularity within a short period of time and the fallout was seen in

[11] This graph was provided by Consumer Sentinel at http://www.consumer.gov/sentinel/Sentinel%20CY-2005/totalnum_ircomplaints&amount.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the lack of policies and laws. Although there are laws in place such as GBLA and Sarbanes Oxley, the unfortunate side is that most regulatory laws do not extend to private businesses. The government sees the best way for privatized business to approach E-Commerce is self regulation. Most say this is because the government is in no hurry to pass legislation. As stated previously in this paper, the best way to protect is through policies and the majority of online businesses do not have such a policies.

There is good news. Even with the lack of government action, the technology that is being created around E-Commerce has a lot of security advances that will help protect consumers and businesses alike. Fortunately, new approaches are being created around infrastructure needs such as application firewalls to protect the code of online applications. This is something that most companies have ignored until now.

What do you do after fraud is committed?

One of the difficult issues for businesses and individuals alike is how to report fraud after it has been detected. Bob Sullivan documented the woes individuals go through when trying to report an incident in his book, *Your Evil Twin.* Sullivan quotes a victim as saying that when she went to the police station to file a report she was laughed at because there was no one to file the report against (Sullivan, pg. 141). The same holds true with merchants that are victims of fraudulent charges.

The best thing to do when faced with the possibilities of identity theft is to notify the three major credit agencies. They offer services for a small fee to monitor any unauthorized activity. This can also be said for any credit cards or banks that the victim may be a part of, as

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

they will be able to offer solutions such as issuing knew account numbers or issuing a freeze.

3. Conclusions

Security Awareness across the Generations

The possibilities for criminals today are endless with all the technology that is available. What most people do not understand is that crimes can be committed simply through social engineering. Social engineering can occur without most people even knowing it is happening. Personally identifiable information is everywhere. It is easily obtainable through intelligent schemes that usually end up with the victim unknowingly giving up the information. The same trend pops up throughout this research paper and it all points back to the information owner.

The ultimate owner of information is the person that has the most vested interest, you and I. Research has shown that businesses and the government are trying to catch up by passing legislation to limit risk. We as citizens need to understand the inherent risk of not taking the appropriate protection measures. While may hold true that businesses should take on the ownership of protecting data, the fact of the matter is they will only do what the law forces them to do. This means we as consumers must control the destiny of the information that is given out and ensure there is proper documentation to protect that information.

The time it takes to recover from an identity theft can be up to six years with tens of thousands of dollars lost in the process. While we have to take a driver's test before driving a car, there is nothing that stops a person

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

from connecting to the Internet. Almost half of the reported data theft scenarios that occur are via the Internet. It would seem if there could be a plan to educate users what not to do that number could be addressed.

Schemes such as phishing, website spoofing and man in the middle attacks can be understood with a simple awareness class. The sad fact is that there will be no wide spread mandatory education anytime soon, but there is a bright side. Major organizations such as Microsoft are beginning to address the technical issues surrounding these online schemes. Windows Vista, the new Microsoft operating system, is going to have a built in feature with Internet Explorer 7 that will automatically detect spoofed internet sites. Symantec now has a built in feature with their Internet Security suite that will scan emails for phishing scams.

Where is the Government in this fight?

The upside is that while there are a large number of identity thefts within the United States, we are better off than most countries. The U.S. government has recognized there is a problem and has begun to enact legislation to help victims recover. They also recognized that businesses need to be more responsible with the information they obtain from consumers. The downside to all of this is that the pace of which they are keeping up with the changing times and advancement in crimes is snail at speed.

Another troubling issue is that the private sector is exempt from most laws that are put into place to help protect consumers. For example, Sports Authority, which has their headquarters based here in Denver, is now going back to being privatized. Why is this? Sports Authority just came out of a major PCI and Sarbanes Oxley audit

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

almost at failures across the board and had to spend millions of dollars to be compliant. The answer to avoiding at least half this "hassle" is of course going private, so that they are self regulated. Self regulation is what fuels this fire of identity theft and needs to be curbed in such a way that there has to be requirements set.

Most states have legislation in place that puts a cap on how many consumers can be affected with a data leak before they have to be contacted. This leaves a loophole for businesses to get out of actually taking responsibility for their unsafe data protection habits. California has it right on this one though with their Senate Bill 1386, which requires notification even if it is only one customer. This should be a bill that is passed at the federal level that forces all businesses to notify customers upon realization of any incident.

Are businesses taking appropriate action?

The answer to this question is two fold mostly because some take it more seriously than others. Corporations can be huge and they still will not have appropriate protection in place for customers or even employees. There are those companies that use their concern for identity protection as a marketing plus. Businesses, whether they are private or public, are taking the wrong approach to this whole situation and here is why. At the end of the day consumers, businesses, and the government are paying billions of dollars to recover from fraud. This has been strictly a mode that is reactive to all situations including taking responsibility. Everyone in this process needs to take an active approach to protection and the businesses need to take the lead. Every business needs to provide a consumer awareness program to anyone that may

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

provide personally identifiable data. This awareness program can take place online before a transaction is made or it can be given in a pamphlet as the customer fills out a hard copy.

Consumer awareness of identity theft and fraud can go a long way to informing people before money is lost on all sides. Information Security awareness is mandatory for employees at most businesses and the same should hold true for the consumers.

Is technology our friend or foe?

The statistics would point that technology is a vehicle for criminals to get away with crimes anonymously. This may be true, but only because the awareness is not out there on how to protect the data in question. There are a wide range of technologies available for consumers and businesses alike to help with protection. Again all signs point back to consumer awareness and education of what products are out there and available.

The up and coming consumer product that is available is a simple form of biometrics. The form I refer to is thumbprint scanning which can be done by a USB device that plugs into a personal computer. The USB device can also store passwords as well as thumbprints for safe keeping. As with all technology though, there are some “gotchas” that go along with it. It was just recently discovered that some USB biometric readers are not actually encrypted properly and can be cracked. Then not only do the criminals have passwords to secure sites but they also have the thumbprint of the victim.

Other forms of biometrics are much too expensive for the average consumer to use and the integration is not there to use with the internet.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The business side of the technology realm is much broader and the protection of data should be paramount. When a consumer gives a business their data it usually ends up in a database with millions of other records. These databases are what pose the most threat to the consumers and even the business that owns the database. There needs to be proper policies put in place that strictly define procedures to protect that data. Surprisingly enough most businesses lack this development of policies leaving data wide open for the taking.

The next thing a business must provide in the way of technology is ENCRYPTION. There are many safeguards in technology, however, with encryption being used in the right instances that is all one may need. A consumer must also know that without encryption over the Internet data is being passed over this huge medium in the clear so anyone can see it. Again, this is where consumer awareness must come in, it seems simple to do. If encryption is not provided between the consumer and the business then the transaction should not take place.

Final Thoughts on Identity Theft

Again I must go back to the fact that a lot of fraudulent situations can be avoided with simple awareness techniques. One would think that by now an Internet user should not click on an email phishing scam link, but that just is not the case. We as consumers must utilize the technology given to us to help fight these online scams and social engineering efforts. The same goes with companies that send out information via hard copy through the mail. A company should not send out confidential data unless it is in a certified mail format.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

This all points back to the policies written, or not written, by each corporation as to how they deal with personally identifiable data. There should be clearly defined standards and process where a company can point back to if there is a question that arises. Policies are the very basis for which consumers and business can agree on how and why they do business.

© SANS Institute 2007, Author retains full rights.

References

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Loberg, K., Son, S., Thorpe, M., & Walsh, James (2004). *Identity Theft: How to Protect Your Name, Your Credit and Vital Information.* California: Silver Lake Publishing

Mendell, Ronald L. (2004). *Investigating Computer Crime in the 21st Century.* Springfield, IL: Charles C. Thomas

Sullivan, Bob (2004). *Your Evil Twin.* New Jersey: John Wiley & Sons Inc.

Vacca, John R., (2003). *Identity Theft.* Upper Saddle River, New Jersey. Prentice Hall

Vaas, Lisa (2005, July 21). Congress Nears Final Identity Theft Legislation, *eWeek.* http://www.eweek.com/article2/0,1895,1839918,00.asp

United States Federal Trade Commission. Consumer Sentinel http://www.consumer.gov/sentinel/trends.htm

ID Theft Resource Center. http://www.idtheftcenter.org/facts.shtml

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**