Global Information Assurance Certification Paper

Computer Security: Informing an Uninformed Public

A look at the home internet user and necessary steps to increase their education

Joseph Sorrenti
GIAC Security Essentials Certification Practical (GSEC)
May 2, 2004
Practical Assignment Version 1.4b Option 1

Abstract

Computer security has come to the forefront of almost every major corporation; even the prime time nightly news carries several stories regarding computer security. However, many home computer users do not have the slightest grasp of basic computer security concepts. They are also unaware of the consequences of the lack of security on their home systems, or why their systems are so attractive to hackers. It is my goal to discuss these issues and possible ways to improve upon them.

Introduction

Computers make life easier. Sharing of files and data are a key part of this concept. "More than half the country's 105 million households have computers, according to U.S Census Bureaus" (Vitale, 2001). Not only do they have computers, but internet usage with those computers is surging as well. According to the Nielson Ratings, "by June 2004 U.S 50% of households will have broadband connectivity with over 75% having connectivity to the internet" (Nielson/Netratings, 2004). Not only is this drastic growth happening within the US, but around the world as well. The following Chart depicts Internet access around the world:

Global Online Populations					
Worldwide Internet Population 2004: 945 million (Computer Industry Almanac)					
Projection for 2005: 1.10 billion (Computer Industry Almanac)		**Projection for 2006:** 1.28 billion (Computer Industry Almanac)		**Projection for 2007:** 1.46 billion (Computer Industry Almanac)	
Nation	**Population** (CIA's World Factbook)	**Internet Users** (CIA's World Factbook)	**Active Users** (Nielsen//NetRatings)	**ISPs** (CIA's World Factbook)	**More Info.**
Afghanistan	27.8 million	NA	NA	1	Read more
Albania	3.54 million	12,000	NA	10	
Algeria	32.2 million	180,000	NA	2	
Andorra	68,400	24,500	NA	1	
Angola	10.6 million	60,000	NA	1	
Anguilla	12,400	919	NA	16	
Antigua and Barbuda	67,400	5,000	NA	16	
Argentina	37.8 million	4.03 million	NA	33	Read more

		(Computer Industry Almanac)			
Armenia	3.30 million	30,000	NA	9	
Aruba	70,400	24,000	NA	NA	Read more
Australia	19.5 million	13.05 million (Computer Industry Almanac)	2.22 million (January 2004, at home)	571	Read more
Austria	8.2 million	4.63 million (Computer Industry Almanac)	1.3 million	37	Read more
Azerbaijan	7.8 million	25,000	NA	2	Read more
The Bahamas	300,500	16,900	NA	19	Read more
Bahrain	656,000	140,200	NA	1	Read more
Bangladesh	133.3 million	150,000	NA	10	
Barbados	276,600	6,000	NA	19	
Belarus	10.33 million	422,000	NA	23	Read more
Belgium	10.3 million	5.01 million (Computer Industry Almanac)	1.6 million	61	Read more
Belize	263,000	18,000	NA	2	Read more
Benin	6.7 million	25,000	NA	4	
Bhutan	2.1 million	2,500	NA	NA	
Bolivia	8.4 million	78,000	NA	9	Read more
Bosnia and Herzegovian	4 million	45,000	NA	3	
Botswana	1.5 million	33,000	NA	11	
Brazil	176 million	23.05 million (Computer Industry Almanac)	12.09 million (January 2004, at-home)	50	Read more
Brunei	351,000	35,000	NA	2	

Bulgaria	7.7 million	1.64 million (Computer Industry Almanac)	NA	200	Read more
Burkina Faso	2.6 million	25,000	NA	1	
Burma	42.2 million	10,000	NA	1	
Burundi	6.4 million	6,000	NA	1	
Cambodia	12.8 million	10,000	NA	2	
Cameroon	16.1 million	45,000	NA	1	
Canada	31.9 million	20.45 million (Computer Industry Almanac)	8.8 million	760	Read more
Cape Verde	409,000	12,000	NA	1	
Cayman Islands	6,200	NA	NA	16	
Central African Republic	3.6 million	2,000	NA	1	
Chad	9 million	4,000	NA	1	
Chile	15.5 million	5.24 million (Computer Industry Almanac)	NA	7	Read more
China	1.3 billion	95.80 million (Computer Industry Almanac)	NA	3	Read more
Colombia	41 million	2.53 million (Computer Industry Almanac)	NA	18	Read more
Comoros	614,000	2,500	NA	1	
Congo, Democratic Republic of the	55.2 million	6,000	NA	1	
Congo, Republic	3 million	500	NA	1	
Cook Islands	20,811	NA	NA	3	
Costa Rica	3.8 million	384,000	NA	3	Read

					more
Cote d'Ivoire	16.8 million	70,000	NA	5	
Croatia	4.4 million	480,000	NA	9	Read more
Cuba	11.2 million	120,000	NA	5	Read more
Cyprus	767,000	150,000	NA	6	
Czech Republic	10.25 million	3.53 million (Computer Industry Almanac)	NA	300	Read more
Denmark	5.4 million	3.72 million (Computer Industry Almanac)	NA	13	Read more
Djibouti	472,800	3,300	NA	1	
Dominica	70,100	2,000	NA	16	
Dominican Republic	8.7 million	186,000	NA	24	
East Timor	952,618	NA	NA	NA	
Ecuador	13.4 million	328,000	NA	31	Read more
Egypt	70.7 million	2.44 million (Computer Industry Almanac)	NA	50	Read more
El Salvador	6.3 million	40,000	NA	4	Read more
Equatorial Guinea	498,100	900	NA	1	
Eritrea	4.46 million	10,000	NA	5	
Estonia	1.4 million	429,700	NA	38	Read more
Ethiopia	67.67 million	20,000	NA	1	
Faroe Islands	46,011	3,000	NA	2	
Fiji	856,300	15,000	NA	2	
Finland	5.2 million	3.26 million (Computer Industry Almanac)	NA	3	Read more
France	59.76 million	26.34	13.78 million	62	Read

		million (Computer Industry Almanac)	(January 2004, at-home)		more
French Guiana	182,333	2,000	NA	2	
French Polynesia	257,800	16,000	NA	2	
Gabon	1.2 million	18,000	NA	1	
Gambia	1.4 million	5,000	NA	2	
Georgia	4.96 million	25,000	NA	6	
Germany	83.2 million	41.86 million (Computer Industry Almanac)	26.66 million (January 2004, at-home)	200	Read more
Ghana	20.2 million	200,000	NA	12	
Gilbraltar	27,700	NA	NA	2	
Greece	10.6 million	3.8 million (Computer Industry Almanac)	NA	27	
Greenland	56,400	20,000	NA	1	
Grenada	89,200	5,200	NA	14	
Guadeloupe	435,700	4,000	NA	3	
Guam	160,700	5,000	NA	20	
Guatemala	13.3 million	200,000	NA	5	Read more
Guernsey	64,587	NA	NA	NA	
Guinea	7.77 million	15,000	NA	4	
Guinea-Bissau	1.345 million	4,000	NA	2	
Guyana	698,000	95,000	NA	3	Read more
Haiti	7 million	30,000	NA	3	
Honduras	6.5 million	40,000	NA	8	Read more
Hong Kong	7.3 million	4.58 million (Computer Industry Almanac)	2.50 million (January 2004, at-home)	17	Read more
Hungary	10.1 million	3.05 million (Computer Industry	NA	16	Read more

		Almanac)			
Iceland	279,000	198,000 (Computer Industry Almanac)	NA	20	Read more
India	1 billion	39.20 million (Computer Industry Almanac)	NA	43	Read more
Indonesia	231 million	15.30 million (Computer Industry Almanac)	NA	24	Read more
Iran	66.6 million	420,000	NA	8	
Iraq	24 million	12,500	NA	1	
Ireland	3.88 million	2.06 million (Computer Industry Almanac)	NA	22	Read more
Isle of Man	73,800	NA	NA	NA	
Islas Malvinas (Falkland Islands)	2,967	NA	NA	2	
Israel	6.0 million	3.04 million (Computer Industry Almanac)	976,000	21	Read more
Italy	57.7 million	28.61 million (Computer Industry Almanac)	15.90 million (January 2004, at-home)	93	Read more
Jamaica	2.68 million	100,000	NA	21	
Japan	127 million	77.95 million (Computer Industry Almanac)	29.95 million (January 2004, at-home)	73	Read more
Jersey	89,775	NA	NA	NA	
Jordan	5.3 million	212,000	NA	5	Read more
Kazakhstan	16.7 million	100,000	NA	10	Read

					more
Kenya	31.1 million	500,000	NA	65	
Kiribati	96,300	1,000	NA	1	
Kuwait	2.1 million	200,000	NA	3	Read more
Kyrgyzstan	4.8 million	51,600	NA	NA	
Laos	5.77 million	10,000	NA	1	
Latvia	2.36 million	312,000	NA	41	
Lebanon	3.6 million	300,000	NA	22	
Lesotho	2.2 million	5,000	NA	1	
Liberia	3.2 million	500	NA	2	
Libya	5.3 million	20,000	NA	1	
Liechtenstein	32,842	NA	NA	NA	
Lithuania	3.6 million	341,000	NA	32	
Luxembourg	448,569	100,000	NA	8	
Macau	461,900	101,000	NA	1	
Macedonia	2.05 million	100,000	NA	6	
Madagascar	16.47 million	35,000	NA	2	
Malawi	10.7 million	35,000	NA	7	
Malaysia	22.6 million	8.47 million (Computer Industry Almanac)	NA	7	Read more
Maldives	320,165	6,000	NA	1	
Mali	11.34 million	30,000	NA	13	
Malta	398,500	59,000	NA	6	
Marshall Islands	73,630	900	NA	1	
Martinique	422,200	5,000	NA	2	
Mauritania	2.8 million	7,500	NA	5	
Mauritius	1.2 million	158,000	NA	2	
Mexico	103.4 million	11.13 million (Computer Industry Almanac)	NA	51	Read more
Micronesia	135,800	2,000	NA	1	
Moldova	4.43 million	15,000	NA	2	
Monaco	31,987	NA	NA	2	

Mongolia	2.7 million	40,000	NA	5	
Montserrat	8,400	NA	NA	17	
Morocco	31.1 million	400,000	NA	8	Read more
Mozambique	19,6 million	22,500	NA	11	
Namibia	1.8 million	45,000	NA	2	
Nauru	12,300	NA	NA	1	
Nepal	25.87 million	60,000	NA	6	
The Netherlands	16 million	10.34 million (Computer Industry Almanac)	7.59 million (January 2004, at-home)	52	Read more
Netherlands Antilles	214,200	2,000	NA	6	
New Caledonia	207,800	24,000	NA	1	
New Zealand	3.9 million	2.34 million (Computer Industry Almanac)	NA	36	
Nicaragua	5 million	20,000	NA	3	Read more
Niue	2,100	NA	NA	1	
Niger	10.6 million	12,000	NA	1	
Nigeria	129.9 million	100,000	NA	11	
Norfolk Island	1,800	NA	NA	2	
North Korea	22.2 million	NA	NA	1	
Northern Mariana Islar	77,300	NA	NA	1	
Norway	4.5 million	3.14 million (Computer Industry Almanac)	NA	13	Read more
Oman	2.7 million	120,000	NA	1	Read more
Pakistan	147.6 million	1.2 million	NA	30	
Palau	19,400	NA	NA	1	
Panama	2.8 million	45,000	NA	6	Read more
Papua New Guinea	5.17 million	135,000	NA	3	

Paraguay	5.8 million	20,000	NA	4	
Peru	27.95 million	2.68 million (Computer Industry Almanac)	NA	10	Read more
Philippines	84.5 million	7.82 million (Computer Industry Almanac)	NA	33	Read more
Pitcairn Islands	47	NA	NA	NA	
Poland	39.0 million	10.6 million (Computer Industry Almanac)	NA	19	
Portugal	10.08 million	6.11 million (Computer Industry Almanac)	NA	16	Read more
Puerto Rico	3.957 million	600,000	NA	76	Read more
Qatar	793,000	75,000	NA	1	
Reunion	743,900	10,000	NA	1	
Romania	22.3 million	3.14 million (Computer Industry Almanac)	NA	38	
Russia	145 million	22.30 million (Computer Industry Almanac)	NA	35	Read more
Rwanda	7.398 million	20,000	NA	2	
St. Kitts and Nevis	38,700	2,000	NA	16	
St. Lucia	160,145	3,000	NA	15	
St. Vincent and the Grenadines	116,394	3,500	NA	15	
Samoa	178,631	3,000	NA	2	
San Marino	27,730	NA	NA	2	

Sao Tome and Principe	170,372	9,000	NA	2	
Saudi Arabia	23.5 million	2.96 million (Computer Industry Almanac)	NA	42	
Senegal	10.589 million	100,000	NA	1	
Seychelles	80,098	9,000	NA	1	
Sierra Leone	5.6 million	20,000	NA	1	
Singapore	4.452 million	2.53 million (Computer Industry Almanac)	956,000	9	
Slovakia	5.4 million	1.82 million (Computer Industry Almanac)	NA	6	
Slovenia	1.9 million	600,000	NA	11	
Solomon Islands	494,786	8,400	NA	1	
Somalia	7.7 million	200	NA	3	
South Africa	43.6 million	5.16 million (Computer Industry Almanac)	NA	150	Read more
South Korea	48.3 million	32.05 million (Computer Industry Almanac)	NA	11	Read more
Spain	40.077 million	16.65 million (Computer Industry Almanac)	8.2 million (January 2004, at-home)	56	
Sri Lanka	19.57 million	121,500	NA	5	
Sudan	37.0 million	56,000	NA	2	
Suriname	436,494	14,500	NA	2	
Svalbard	2,868	NA	NA	NA	
Swaziland	1.1 million	14,000	NA	6	

Sweden	8.9 million	6.12 million (Computer Industry Almanac)	4.56 million (January 2004, at-home)	29	Read more
Switzerland	7.3 million	4.68 million (Computer Industry Almanac)	3.07 million (January 2004, at-home)	44	Read more
Syria	17.15 million	60,000	NA	1	Read more
Taiwan	22.5 million	13.20 million (Computer Industry Almanac)	5.0 million	8	
Tajilistan	6.7 million	5,000	NA	4	
Tanzania	37.18 million	300,000	NA	6	
Thailand	62.3 million	8.42 million (Computer Industry Almanac)	NA	15	
Togo	5.285 million	50,000	NA	3	
Tokelau	1,400	NA	NA	1	
Tonga	106,100	1,000	NA	2	
Trinidad and Tobago	1.163 million	120,000	NA	17	
Tunisia	9.81 million	400,000	NA	1	
Turkey	67.308 million	6.82 million (Computer Industry Almanac)	NA	50	Read more
Turks and Caicos	18,738	NA	NA	14	
Turkmenistan	4.6 million	2,000	NA	NA	
Tuvalu	11,100	NA	NA	1	
Uganda	24.7 million	60,000	NA	2	
Ukraine	48.39 million	2.81 million (Computer Industry Almanac)	NA	260	

United Arab Emirates	2.445 million	900,000	NA	1	Read more
United Kingdom	59.8 million	34.11 million (Computer Industry Almanac)	20.87 million (January 2004, at-home)	<400	Read more
United States	280.5 million	185.90 million (Computer Industry Almanac)	141.02 million (January 2004, at-home)	7,000	Read more
Uruguay	3.386 million	690,000 (Computer Industry Almanac)	NA	14	Read more
Uzbekistan	25.563 million	100,000	NA	42	
Vanuatu	196,100	3,000	NA	1	
Venezuela	24.287 million	3.04 million (Computer Industry Almanac)	NA	16	Read more
Vietnam	81.098 million	400,000	NA	5	
Virgin Islands	123,498	12,000	NA	50	
Wallis and Futuna	15,500	NA	NA	1	
Western Sahara	256,177	NA	NA	1	
Yemen	18.701 million	17,000	NA	1	Read more
Zambia	9.959 million	25,000	NA	5	
Zimbabwe	11.376 million	100,000	NA	6	

Chart inserted from (ClickZ Stats staff, 2004).

The internet is based on sharing of resources and security is based on limiting access to those shared resources. It becomes a delicate balance that is not so clearly defined or easily administered. With all this connectivity and increased capacity, security must be brought to the forefront of the home users minds.

The Issue

When you're involved in the IT field, you become the IT guru for everyone of your friends and family members whether you like it or not. In assuming this role it became clear that computer security was not making its way into the homes/ practices of everyday people. Several months ago a close associate of mine who is extremely reserved and private particularly with his personal information, signed up for an online account. Several minutes after his initial login, he received an email stating it was from the ISP (Internet service provider) customer service asking him to provide his credit card information again. He obliged without thinking twice about issuing sensitive information via email. He later received another email claiming to be from a different customer service rep asking to verify the credit card address. This is when I received a call asking if this was normal. I informed the person to call his credit card company and have the card suspended. It turned out there was already over $2000 in fraudulent charges. In another incident another associate recently installed a broadband router. I received a call stating his system would no longer function. After a brief visit it turned out he purchased one of the install it yourself packages for a discount and didn't bother to add any security features. He assumed the antivirus was enough. (Anti-virus that came with the system and had expired months ago). Needless to say, the system was compromised by spy ware, several of the latest virus programs and a hacker. After several hours of work, a software and hardware based firewall install, a spy ware removal tool and the latest antivirus software, the system was usable again. My associate passed a comment, "it would have been easier and cheaper to toss the compromised system and purchase a new one." He was probably right, but that is not always an option. These are just two of my most recent experiences with home users and security issues. I've come across many more over the years. In attempting to ascertain why someone with reasonable intelligence would install something without taking basic precautions the answers I usually come across are "I just assumed it was safe or why would they sell you this stuff and not tell you what to beware of". There is a general association being made, because something was bought from a trusted source, the device, item being purchased is automatically trusted. Think about your friends, family, and associates. How many of them have fallen into a similar situation? Think about your accountant doing your taxes on his brand new wireless laptop that has not been secured in any way. This is a concern worth paying attention to which is exposed by the following excerpt taken from the Identity theft resource center, facts and statistics; "More than ever, the information explosion, aided by an era of easy credit, has led to the expansion of a crime that feeds on the inability of consumers to control who has access to sensitive information and how it is safeguarded. That crime is identity theft. According to 2 studies done in July 2003 (Gartner Research and Harris Interactive), approximately 7 million people became victims of identity theft in the prior 12 months." (Identity theft resource center, 2003)

In the information technology industry much emphasis is placed on getting the software manufacturers to build better security into their products. I'm not suggesting we shy away from this, what I am suggesting is doing more on the consumer side. Corporations responsible for selling consumer products should

educate the consumer about the perils of lax security. When was the last time you entered a Best Buy or Sears and saw an Internet related product touting its security benefits. Even commercials for broadband access tout speed and reliability, what about security?
It shouldn't be difficult to educate the consumers; comparisons such as buying a house could be used. One of the first things a person does when purchasing a new home is change the locks on the exterior doors, yet this same person who buys a wireless router not only doesn't check the locks, but also leaves the defaults settings in place. They are usually happy it just "worked". When a computer system is compromised, more than just the owner of that system is at risk. The compromised system can and is used many times to launch attacks on other systems primarily in the corporate world or even internationally.

The International question:
One day at work I was noticing persistent attempts to gain access to my network via our firewall. I began to hunt down the offending address and traced it to an ISP in another country. When I attempted to ascertain the identification of the offending IP address I was emailed a statement stating; "Please note, we are not allowed to publish any connection records or user information… since they must obey their specific countries laws. To obtain the information I must obtain a judicial decision from their country, by logging a complaint with the proper authorities within their country." They didn't make it easy did they? Odds are the offending address belonged to some person out there whose computer was compromised. There are many countries listed in the above Internet access chart that do not have the best interest of the Unites Stated at heart. A good example of this is in the article written by Adam Piore for Newsweek International. In it he states;

> "Hacking into the U.S. systems isn't illegal in Russia. The lack of anti hacking laws is not unique to Russia. China's laws regarding cyber crime are inadequate, say officials. Brazil's legislation provides for paltry incarceration rates and enforcement is lax. The EU has drafted laws similar to those in the Unites States but has yet to ratify them. "Piore goes on to add; "What can companies and home-computer users do to protect themselves? Vigilance is the only option. Corporations—particularly small- and medium-size ones—could do better at availing themselves of new software that plugs security holes in antiquated servers, such as new products introduced last year to deter certain kinds of spoofing scams. And whereas large corporations generally hire security experts to scan their software and computers to make sure that any backdoor administrative passwords are deleted, most small- and mid-size companies don't bother. Individual computer users can be even more vulnerable. "There are so many industry-best practices not being implemented by home users," says Dartmouth's Bakos. Among the recommended practices are using firewalls and security software. Says Lee Byong Ki, police chief in charge of cyber crimes in South Korea: People "need to understand that as soon as their server is connected to the Internet, their information is exposed to hacker attacks." (Piore, 2004)

The key point Piore makes is pointing out the statement by Dartmouth's Bakos. There are already industry-best practices, but how do you present those practices to those who are not in the industry? Helping to educate home users on the perils of poor computer security and industry-best

practices would greatly reduce the risks not only to the user themselves, but to our country as a whole. With terrorism being what it is today, securing our Internet borders should be treated as a critical issue.

Possible solutions

Education
In my opinion, education is one of the primary cornerstones of society. It becomes the key factor to winning this battle. The same items that are discussed in the Sans Giac and most other security courses need to be presented to the home user in a "user friendly" approach that is extremely affordable. Another way of looking at it is to take our corporate policies and create a generic every day home user policy. This should be a uniform policy and presented within the packaging of every single vendor product sold to home users.

The following topics should garner attention:

- Email:

Opening unknown attachments: Basic principle of if you do not know the sender or did not request the attachment do not open it.

- Encrypting: Sensitive data should be encrypted prior to being sent over the internet. Examples would be medical records, Credit card numbers, applications

- Antivirus software: all home systems should install a subscription based automated update antivirus software linked to the users home email client.

- System Patching: Automated tools should be installed to ensure all the latest vendor patches are applied to a home system.

- Firewalls: If system is connected to internet a Host based Firewall (software) should be on the system, if possible a network based state full packet device as well

- Passwords: User password should be used and changed monthly at minimum. Standard words should be avoided and alpha numeric characters should be encouraged.

- Basic Wireless Security: WEP (wireless encryption should be used) Default SSID should be changed and not broadcasted. If possible, MAC address filtering and additional authentication methods should be used.
- Browsing
    - Proper site verification: Understanding how to verify sites visited as well as ecommerce trusted sites is critical.
    - SSL encryption – Any site which requests personal information should at minimum be encrypted with 128 bit SSL
    - Visiting sites: Don't just assume all sites are valid and safe, know where you are traveling. It's the same as driving in a car, you avoid the dangerous areas of town; the same rules should apply to the internet.

- Backups: All essential data on a home users system should be backed up to a separate location or media if possible.

The above bullet points by no means represent a thorough policy, rather a starting point for further discussion. A solid resource that goes into a majority of these points in more detail can be found at:
http://www.isalliance.org/resources/papers/ISAhomeuser.pdf

Legislation

All these possible compromises bring to mind the question, who is responsible? The unsuspecting user who uses the defense; I didn't know?" Other areas of our society, the law states ignorance is not a defense – Are the hundreds of users whose computers been compromised at legal risk? So far this defense seems to be holding at lease in the UK where it was first used;

"Aaron Caffrey, 19, was accused of crashing systems at the port of Houston in Texas by hacking into its computer systems. But a jury cleared him after believing his defense that hackers had broken into his computer and used it to launch the attack. "This verdict sets a potentially dangerous precedent with regard to hacking cases," said Cable & Wireless security expert Richard Starnes. "(BBC News, 2003).

As you can see it has already raised questions from some in the security field. Will it eventually be necessary to insure your computer as you do a car for liability? Currently corporations that are compromised are assuming the cost of burden. It will be a matter of time before large corporations begin to look for financial restitution from the last known source point of the attack. This would surely have the effect of having users pay more attention to security. In other areas of our society, If you own a gun and leave it unlocked or accessible and it is used in a crime, in certain states you can be charged as an accomplice, as cited on the Brady center to prevent gun violence, the; "The Court held, "Guns are dangerous instrumentalities that in the wrong hands have the potential to cause serious injuries. It is a responsible gun owner's duty to exercise reasonable care in the safe storage of a firearm" (**Estate of Heck v. Stoffer**, No. 02A03-0007-CV-267, Supreme Court of Indiana).
Can those same arguments be applied to a home user system that may have caused a company to go bankrupt due to stolen secrets, or a hospital system that has been compromised and patient's medication altered causing a death? At some point in time legislation will become necessary to resolve most of the issues. We live in a reactive society; laws are generally created after a dispute or large catastrophe. I believe if we do not begin to educate the home user ourselves the government will eventually step in.

Licensing

Licensing is available for many different things. Driving a car is one that most of us are familiar with. When cars were first introduced as a new technology licensing was not around, as the technology grew and was adopted licensing was needed to make sure that safety, accountability and reliability became the standards of driving. The same argument can be made for the licensing of computers. At minimum an acknowledgement of a home user policy should be discussed. The homeland security department could be responsible for administration of the policy. Computers can and have been used a weapons against our country, corporations and selves. Shouldn't that warrant the level of interdiction that entails licensing?

Personal Responsibility

It takes initiative and willingness to learn about systems vulnerabilities, patch them and continually update them. Again, I go back to the car analogy; occasionally a defect will occur on a certain model car. The manufacturer sends out a notice to the dealership as well as the last known owners. It is then the owner's responsibility to bring the car to the dealership for proper repair. In the case of computer system and or device, an email or letter may arrive, and it would be the home owner's responsibility to visit the company's site and download and install the latest patch. Many businesses, schools and not for profits make end users sign agreements that state the user is responsible for all actions while on their network. Can an ISP agreement monitored by a government agency enforce that same type of agreement? On-line banking is another area which poses significant threat. Banks are liable for losses to accounts, but the question has been raised regarding customer responsibility. "Roland le Sueur, the head of internet banking at First National Bank, says the bank cannot be held responsible for what happens on your personal computer. Just as the bank takes responsibility for the security of its system, consumers must be responsible for the security of their PCs" (Clayton, 2003). If the responsibility of the system belongs to the user, then the financial loss should as well.

Third party Groups

There are some organizations trying to bring security issues to the forefront of society. One group is PFIR (People for Internet Responsibility). They are a group whose;

"Ultimate goal of the conference is to establish a set of **specific** actions and contingency plans for the Internet-related problems that could lead to the meltdown. These may include (but are not limited to) technical, governance, regulatory, political, and legal actions and plans. Scenarios to consider may also include more "radical" technical approaches such as "alternate root" domain systems, technologies to bypass unreasonable ISP restrictions, and a wide range of other practical possibilities." (PFIR, 2004).

This group doesn't look to educating the user, rather they recognize the potential for disaster and attempts to bring attention to security issues via corporations and sponsors and media. I'm not too sure of the effectiveness of this approach as we

are several years into the technology age. Yet, many who consider themselves computer literate are still computer illiterate when it comes to security.

Organizations such as CERT carry information on Home network security. See http://www.cert.org/tech_tips/jome_networks.html they offer very informative documentation, but it contains technical jargon that can scare most home users away.

Search engines such as google are also a tool which can be used to find information regarding computer security for home systems.
The information is out there, it is just a matter of getting it into the right hands again because it's worth repeating, in a "user friendly" format.

Conclusion

A lack of education regarding home user computer security can create problems ranging from corporate bribery, to personal identity theft, to a threat for national security. Hackers are interested in systems for many reasons, some of the more prominent ones being:

- System resources: they are after the raw processing power of the computer
- System files: they want access to files for credit card numbers, passwords etc.
- Curiosity: because it is there
- Acknowledgement: some do it to show off or look for praise from their peers

Personal responsibility, education along with legislation and possibly licensing are the keys to helping provide a safer secure networked environment. Corporations who provide computer related products to consumers must take a lead role in producing and prominently displaying security concerns. Scripts should be created to ease the implementation of security features for those not in the technology field. Education not only from those within the Information technology field, but news organizations, corporations and individuals need to play more of a role in ensuring a better secure environment. The news organizations within the media can begin to play a larger role by creating more specialty segments. Legislation can help to assure standards are met and followed and licensing can be used to assure a minimum set of standards has been applied. Government and third party intervention can help play a role, but the general philosophy of the openness of the Internet creates a substantial debate regarding governmental regulation. No one item taken alone can be successful; a coordinated effort is needed to assure a safe healthy environment going forward for all. The Internet has to evolve with the growing threats it faces. If it doesn't, like all previous failed products, it doesn't matter how useful something is, if the risk out weights the advantages, it will eventually fail. The more we as a society rely on the Internet, the more we will be lost without it. The

loss of dollar amounts due to intrusions keeps getting higher; "A survey by the U.S. Federal Bureau of Investigation (FBI) and the San Francisco-based Computer Security Institute (CSI) found that Internet security breaches are getting costlier as theft and intrusion become more widespread and sophisticated…. The survey of 538 U.S. computer security companies and government agencies found that 85 percent detected security breaches in the last year and 64 percent acknowledged financial losses because of theft or attack. The average annual loss in the three years prior to 2000 was about US$120 million, according to the survey" (Lyman, 2001). With more and more corporations securing their internet borders hackers are going to look for different targets. Those targets are going to continue to be the uninformed home user.

References

Vitale, Madelaine. “More than half U.S. households own computers, census shows “ The Press of Atlantic City.
URL:http://www.ettc.net/press/households.htm

Nielson/NetRatings.
URL:http://www.netratings.com/pr/pr_040318.pdf

ClickZ Stats Staff. “Population Explosion”
URL:http://www.clickz.com/stats/big_picture/geographics/article.php/5911_151151

Identity Theft resource center. “Facts & Statistics”
URL:http://www.idtheftcenter.org/facts.shtml

Piore, Adam. “Hacking for Dollars”
Newsweek International
URL:http://msnbc.msn.com/id/3706599

PFIR “People For Internet Responsibility”
URL: http://www.pfir.org/meltdown

Lyman, Jay. “U.S.: Cost of Hacking Skyrockets”
URL: http://www.newsfactor.com/story.xhtml?story_id=8117

BBC News. “Questions cloud cyber crime case”
URL: http://news.bbc.co.uk/2/hi/technology/3202116.stm

Brady Center to Prevent Gun Violence. “**Estate of Heck v. Stoffer**, No. 02A03-0007-CV-267, Supreme Court of Indiana”
URL: http://www.gunlawsuits.org/docket/casestatus.asp?RecordNo=73

Clayton, Charlene “Your PC, your responsibility, says banks”
URL: http://www.persfin.co.za/index.php?fsectionId=5928&fArticleId=196530

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event