Personal Protections in Cyberspace

The internet is a battlefield on which individuals are increasingly at risk. Individuals are the source of personally identifiable information and the victims of thieves, hackers, and organizations who access and misuse their data. Like corporate and National Defense program managers, individuals are being lured by the Sirens of convenience, speed, and social connectedness. The purpose of this paper is to raise consciousness of the threats to individuals and the power they have to better protect themselves in cyberspace. Defenses and actions by individuals to reduce and harden their cyber footprints are underutilized and essential to identity protection. But neither cyber security nor education on inherent risks and related defenses have kept up with the pace of cyberspace development and use.

Our appetite for the speed, connectivity, and conveniences of cyberspace has resulted in a mad rush to place our systems and processes on-line, whether they are personal, business, or National Defense systems. Yet risks to confidentiality, integrity, and availability of our data, processes, and systems are not fully understood and are accepted casually.

Personal information is controlled in the three spaces that comprise cyberspace; System Space, Organizational Space, and Personal Space. System Space is comprised of computer hardware, software, network devices, and interconnections that make up the internet. Organizational Space is comprised of government and organizational laws, policies, and process, along with their implementation. Personal Space is comprised of an individual's digital identity and digital persona; user names, e-mail addresses, social media profiles, identity tokens, icons, avatars, data, and transactions.

Personal Threats

System Space Threats. Threats in the System Space are connectivity related, connectivity being an innate characteristic of cyberspace. Computer systems connected to the internet cannot be completely hardened with information assurance protections. Such protections do raise the bar of sophistication necessary for penetration. But the only way to completely isolate a network or system from the threats in cyberspace is to disconnect it from the internet. However, even then internal threats persist. Systems can be penetrated, altered, and shut down. Denial of service attacks can overwhelm system bandwidth and cut them off from their users.

Organizational Space Threats. Threats in Organizational Space emanate from the adequacy and equally important implementation of laws, regulations, and guidance. Countries are currently struggling with crafting laws that protect their citizens and at the same time fit with the laws of other countries. Laws concerning ownership of your personal information, information retention periods, and citizen's rights along with their implementation can threaten individual privacy and control of personal information. As important as the laws and regulations themselves is how they are interpreted and implemented. Organizations frequently lack rigor in implementing even minimal standards for information assurance. The Department of Defense Inspector General recently reported weaknesses in protecting Privacy Act information found in

42 audits conducted during the last year by them, the Naval Audit Service, the Air Force Audit Agency, and the Government Accountability Office. The audits clearly show that organizations are not adequately implementing information assurance regulations.

Classified corporate and government information has been stolen and leaked. Sensitive and valuable strategies, tactics, research and development results, and operation information have been stolen, altered, and destroyed. Healthcare breaches cost the industry billions of dollars each year and are on the rise. Trusted relationships, a pillar of corporate and government ability to function, are being tarnished. National infrastructures are subject to internal, foreign, and terrorist cyber war attacks; as examples, the Illinois water utility and the Iran nuclear reactor.

Organizations continue to centralize and automate their systems, increasing the potency of cyber attacks. National Defense, financial system, infrastructure, and organizational nodes are thus created that can be targeted as single points of failure. The results of attacks on organizations ultimately translate to threats on individuals.

Personal Space Threats. Threats in Personal Space are directly tied to individuals' control, release, and management of their personal information, as well as how their information is handled in the System and Organizational Spaces. Individuals, the source of personal information, are also the main victims of identity theft and hactivism. Yet individuals are putting their personal information into cyberspace with abandon and at an expanding rate, even though laws and regulations are not always slanted in their favor and organizations seldom achieve minimum standards of information assurance.

People voluntarily provide just about everything about themselves to systems in cyberspace. The following chart, Personal Artifact Collection Points, lists some of the places people contribute or leave personal artifacts.

Current and past cell phone and GPS device locations	Security badge check points	Credit Reporting Agencies
Medical Records	Doctors, drug stores, and Companies	Drivers' License and Motor Vehicle Bureaus Records
Real Property transactions	Voters' Records	Passport Records
Financial Institutions	Automatic deposits	Scheduled payments
On-line banking	Web bill paying	Credit card applications and use
Mortgage loans	Car loans	Gas and store credit cards
Telephone records	Internet service providers	Utilities
Search Engines	Trackers on your computer	Data Repository Organizations
Address confidentiality	Information Brokers	Trip Passes
Social networks and Fake Social Networks	Hotel reservations and programs	Airline, train, rental car companies
Travel companies	Restaurants	Commuter passes
Toll road "Smart Passes"	Grocery and other store cards	IRS

Parking passes & credit card parking meters	Insurance accounts	Bank accounts
State and local Tax Commissions	Professional organizations	Academic records
Any on-line service	Fraternities and sororities	Police and court records
Charity organizations	Surveys	Medical records
Employee Personnel Records	GPS devices	
Signal emitting cards		

Chart. Personal Artifact Collection Points

Digital persona information can be, and is being, obtained, stored, and collated in ways that can empty bank accounts, influence hiring, get people fired, and taint reputations. The news media is increasingly filled with accounts of fraudulently obtained and abused account numbers pass words, addresses, and drivers' license numbers. The information is being used for fraudulent charges, spam campaigns, and other personal attacks. But not captured by the news media is the cost to individuals in terms of time loss, wealth loss, reputation tainting, and mental anguish.

Hactivist groups collect data from multiple sources, collate it, and then "out" the data in attacks on targeted individuals and their family members. The vicious attacks cause extreme financial and personal damage that can effectively neutralize a targeted employee from performing his function.

An individual's immediate whereabouts can be pin pointed, along with past movements. Utility usage data can be used to identify patterns of home vacancy and vulnerability. Civil rights groups want to have the retention of an individual's location information limited. But law enforcement agencies find such information very "useful" and prior to a recent Supreme Court ruling used GPS tracers without warrants.

Personally identifiable information in corporate credit card data bases, search engines and social sites is being subjected to data mining techniques to discover and identify social, consumption, and criminal behaviors. Our personal data are also being used to shape our attitudes and consumption preferences. The psychological, sociological, and ethical implications of this social engineering are not yet known and will be the subject of extensive, future studies and analyses.

The value of personal information is illustrated by Wall Street in its valuation of companies whose primary asset is the possession of and access to large collections of personal information. Individuals are volunteering the rights and ownership of their personal information to gain access to internet applications, make purchases, transact business, and perform queries. Look carefully at the long, boiler plate agreements that are required by web sites. If we don't agree to them, we are denied access. The data collectors, not we, end up owning our personally

identifiable information. Our children are growing up with on-line legacies of all of their sometimes silly and ill thought out inputs, no longer in their legal possession or in their control to delete.

Personal Protections

System Level Protections. Personal information is only protected at the system level to the extent that implemented information assurance has raised the bar of sophistication necessary for penetration. Even isolating a network or system from the internet will leave exposure to the internal threat.

Organizational Level Protections. Personal information protection at the organizational level is comprised of policies found in national and international legislation, regulations, standards, and guidance along with the all important interpretation and implementation of the same. Lawmakers and administrators continue to generate more laws requiring information assurance and audits continue to find that organizations are not adequately complying with those already in place. Existing policies include:

- The Privacy Act of 1974, 5 U.S.C. § 552.a, which states in part:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of the individual to whom the record pertains, unless disclosure of the record would be – … . [A list of exceptions is thereafter provided].

- The Federal Information Security Management Act (FISMA) of 2002, which provides "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."

- The National Institute of Standards has issued more than 300 information security documents including their Federal Information Processing Standards (FIPS) that relate to the Federal Information Security Management Act (FISMA) of 2002.

- The Department of Defense Privacy Program, DoD 5400.11-R of May 14, 2007, which states in part:

> DoD Components shall establish appropriate administrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

- The Department of Defense manages their information enterprise with their DoD 8000 series of Directives and Instructions.

- Some organizations have regulations that provide for the protection of a select few of the top officials. The regulations that allow expenditures for the protection of lower level employees require justifications and reviews at multiple high levels. It appears that most employees who suffer an identity theft or a hactivist attack will not receive such protection.

Recent national policy initiatives include:

- Senators Lieberman, Collins, Rockefeller, and Feinstein introduced the Cyber Security Act of 2012. A cursory review of the proposed tome reveals a focus on the organization space, including its provision for establishing "… a cyber security awareness and education curriculum that shall be required for all Federal employees and contractors engaged in the design, development, or operation of an agency information infrastructure or the Federal information infrastructure." The proposed curriculum does include one identity item called "identity management information."

- The White House issued a new Consumer Privacy Bill of Rights in February 2012: CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY. Although the document is only guidance, the President did state that he is rejecting "the conclusion that privacy is an outmoded value" and that his "Administration will work to advance these principles and work with Congress to put them into law." One of the most encouraging principles of the document is "1. INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it."

- One tool whose legality is being debated is mitigative counter striking. The defense entails detecting and tracing an intrusion and executing a counter strike. The approach is sort of like ensuring peace by giving everyone a gun. But offensive cyber weapons are on the scene. Of particular note at the National Defense level is the cyber offense capabilities of China.

Other countries and their organizations are also actively crafting policies to protect their citizens. Identity protection, like cyberspace itself, is a worldwide issue. One interesting example is Argentina's "Right to Be Forgotten" law that gives individuals the right to require internet companies to remove specific personal information. It has already been used by a celebrity to require the removal of a photo. The law is also being considered by the European Community countries. The concept of such a protection for individuals is drawing the ire of proclaimed free speech advocates. Such legislation would also be of great concern to those internet companies whose fortunes are built on collections of personal information. The complications and conflicts of national laws in the international space are of great concern to internet companies who operate in multiple countries.

Personal Level Protections. Personal level protections are those actions that individuals can take to protect themselves. They are many and grossly underutilized, possibly due to individuals being uninformed. One of the most effective initiatives to protect identity would be a massive educational movement to ensure that individuals understand the seriousness of the threat, carefully control what personal information they give away, and actively monitor their digital persona.

In addition to understanding the personal hazards of cyberspace, individuals need to know specifically what actions they can take to protect themselves. A partial list of information that needs to become common knowledge includes:

- How to contact the three credit agencies and freeze access
- How to obtain and review medical reports for tampering and accuracy
- How to instruct the DMV to restrict sharing records
- How to contact state and local governments and their agencies to restrict information release and advise you of unauthorized access.
- How to review your monthly credit card statements
- How to generate good passwords and not reuse them for multiple accounts
- How to ensure you have set up internet service provider restrictions
- How to educate your minor children on what not to share on social networking sites
- How to surf the web anonymously
- How to detect and to whom to report intrusions
- How to respond to identity theft

Conclusion

Identity threats and risks from the internet and our relationship with it will not be eliminated. But the risks can be reduced by continued efforts in system, organizational, and personal spaces. One of the most effective and badly needed initiatives would be a grass roots movement of self protection. Knowledge of the hazards of cyberspace and specific actions each individual can take needs to become common knowledge. The internet battlefield would look a lot different if every individual reduced and hardened his or her digital foot print.