GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Ron Bilberry
GSEC Practical Assignment version 1.2b

Security versus Privacy – Whose move is it?

Somewhere within the vast outline of this game, we call Information Technology; there is a balance between security and the privacy of personal data. The winners of the game will find that balance and thereby secure their customers confidence and increase their market share. However, the game rules are not explicit and only now are being defined by the rule makers.

George Orwell's novel "1984" presented a world of totalitarian images of the Ministry of Truth, the Thought Police, and the notion that Big Brother was always watching every citizen. I wonder if George Orwell could have imagined our present situation. Many Americans are concerned that their personal data is being stored in databases and utilized in ways that they never intended. While other "entities" are worried that the use of those databases is about to be curtailed by required compliance with new legislative measures.

According to Citizens Against Government Waste,**1** " the average American has personal, financial and work-related data documented by the federal government in databases, that cover everything from Social Security information to student loan records to applications for mortgages." Not only does the Federal Government store sensitive data on it's citizens, but many Corporations contend that their continued success requires them to gather and distribute personal data, largely unknown and unseen by the public. The information gleaned from public records and retail databases can include demographics including income, size of family and lifestyle interests.

Profiling of consumers has become an integral part of retail business, providing marketing firms the ability to target prospects of almost any product. Most people will not object about the information they provide while completing a transaction. The amount of data gathered, when a new catalog, free download or newsletter is offered to the unsuspecting, can become very extensive. Marketing organizations insist that consumers will see costs go higher if this type of data profiling is prevented.

Other intrusions on privacy have been in place for years without protest by citizens. It has been reported that the average New Yorker is photographed something like 23 times a day by video cameras in stores, offices and public buildings or by traffic cameras on the street. When cameras on traffic lights were installed to catch reckless drivers, it was for the benefit of society at large. Some people welcome these intrusions as being more beneficial than harmful. **2**

In the near future, young people having grown up with new technologies will not even consider if privacy was lost or security gained. Today a Global Positioning Satellite system can provide worldwide tracking. "Always –on " communication would keep you

© SANS Institute 2000 - 2005 Author retains full rights.

connected to the office or home. It is predicted that 40% of adults and 75% of teens will have some type of wearable, always on computing and communicating device within 10 years. When a wireless messaging service called Short Message Service became available in Finland, teenagers integrated it overnight into their social life. Staying in touch with peers and friends became expected, part of "being there." Web cameras have appeared throughout the Internet world and hundreds of individuals offer an intimate view into their lives via web cams. " Smart tags" installed on vehicles can allow one to drive through tollgates without slowing down. Does this mean the government has the potential to track your movements? Franklin Reeder chairman of the Computer System Security and Privacy Advisory Board says," It comes down to individual perceptions. What constitutes an invasion of privacy to one person is a welcome convenience to another. What is important here is choice, he says. Those who want the convenience can opt in: those who see it as an intrusion " simply don't get the smart tag." **2**

Surveys conducted by TRUSTe, an independent, non-profit privacy initiative, show that " loss of personal privacy" was a top concern of Americans for the new century. Among Internet users, 37% indicated that they would be more inclined to purchase from a site that has a privacy policy. Privacy/Security is the #1 factor that would convert researchers into buyers, as reported by 68 % of those surveyed by Jupiter Communications, 6/99 **3** Many concerned individuals refuse to release information over the Internet if they cannot be assured of the security and authenticity on the opposite end of the wire. Some would refuse to use new technologies if they cannot be certain of privacy. "While the Internet / eCommerce industry is built on trust between businesses and customers and given that privacy is the number one ingredient in trust. Unless we can address the issues of privacy and security of data, the Internet companies will lose the trust and thereby the business of their customers."**3**

At Computer World's Premier 100 IT Leaders Conference, a panel of members acknowledged that security and privacy is also a problem for senior management. Lack of awareness and preparedness has caused alarms to sound throughout corporate America. Executives have been caught off guard, being unprepared could contribute to financial losses and legal troubles for companies that fail to address security. Privacy regulations relating to the protection and use of confidential personal information about customers are requiring changes in corporate culture. Surveying those in attendance, a poll found that 56% said that executives at their company have " no clue" to understanding the relationship of IT security and the potential for financial or legal disaster. Only 18% said that their management teams were "very aware." **4**

Privacy and security have become hot issues, which is evident by the activity seen at National Conferences and the amount of legislation before Congress. Over 40 bills have been introduced to the 107th Congress this year. Some regulations have already become law, Health Insurance Portability and Accountability Act (HIPAA), concerning patient's medical records and the Graham-Leach-Bliley Act for deregulation of financial organizations. These recent regulations are still being debated, even though Congress has

© SANS Institute 2000 - 2005 Author retains full rights.

already enacted both into U.S. law. Some type of Federal "online privacy " law is thought to be ready now, even though questions about cost, compliance, and disparity remain. On the state level twenty-eight states have some type of privacy protection in place and those that do not have one today, probably will before the end of 2002.

Issues that are being disputed within the proposed legislation include:

1. Whether customers can select an "opt-in" versus "opt-out " for e-mail advertisements. Consumer groups desire to "opt-in", while business groups contend that would prevent their ads from reaching consumers if they had to choose.
2. Allowing customers to have access to information collected by a company. Privacy groups insist that access is a fundamental right.
3. Federal Preemption. Congress could override state privacy law and limit a person's ability to sue, as it did with Y2K liability legislation.

The Texas State Legislature is considering House Bill 1922, entitled "State Government Privacy Policy." It will recognize the right of individuals to make corrections and that those procedures will not unduly burden the individual. HB 1922 also would entitle an individual to be informed about information that a state governmental body collects about the individual.

However, would these laws provide the right solution? What could be wrong with the Congress proceeding with new regulations and the states forming their own? If the public is demanding protection of information and security of data; wouldn't that also be good for IT. The Corporate Board rooms have been warned. Lawsuits by damaged parties and decisions handed down by Federal Courts could seriously impact their business with monetary losses.

A study of the costs involved in just bringing the present websites of US companies into compliance with proposed laws is estimated from $9 billion to $36 billion, according to a recent study by the American Enterprise Institute-Brookings Joint Center for Regulatory Studies. **1** Small businesses would be hardest hit, the costs of compliance would be substantial, taking a severe hit on the economy and still not meeting all concerns of consumers. Compounding the problem will be the patchwork of state laws being passed. More than 450 privacy–related bills have been introduced in the state sessions within past years, while Congress has before it 40 or more privacy bills today. Making all state laws and federal laws standard would help, but that is not expected and would still take a long time. While America is looking to Information Technology to continue its expansion and growth to fuel the rest of the economy, compliance required by these regulations would be a heavy blow. The European countries have already enacted legislation requiring compliance and cooperation among their members. They have been waiting for US companies to join with them, however many US Executives contend that the European agreement is too confining and extensive for US businesses.

© SANS Institute 2000 - 2005 Author retains full rights.

The Federal Trade Commission has said that companies need to standardize privacy policies, utilizing clear wording. FTC Commissioner Sheila Anthony was reported to say, "Companies need a standardized policy much like ingredient labels found on food products." **5** However, other Industry experts point out that the FTC is limited in what it can do to make companies improve. Other experts point out that many agencies within the Federal Government have failed to comply and standardize upon security guidelines.

In April of this year, it was reported that the General Accounting Office had penetrated and secured access to sensitive data on the Internal Revenue Services computers. **6** Those computers contained personal data from 35 million taxpayers, stored in plain-text files. Basic security flaws were found throughout the IRS e-file system. The IRS contends that no hacks have been detected outside of the GAO's; however, at the time there were no procedures in place to detect such attacks. Unfortunately the IRS is not alone, many government agencies and private companies have experienced intrusions and hacks to their systems. It is certain that more intrusions and loss of data will continue. Furthermore, it is believed that less than 50% of attacks, intrusions, hacks and loss of data are being reported.

So if compliance with multitudes of regulations is going to be too expensive, if it will cost billions in revenue and if the Federal Government cannot agree upon a standard policy or enforce those guidelines; much less make it's own systems secure, how can Information Technology solve this dilemma? Whose move is it? First off, we must not wait for legislation. We must take the initiative ourselves to make self-regulation and security of data first priority. Revealing personal data in exchange for something received has not been found to be problematic to most Americans. Many have already resolved the trade-offs between convenience and privacy. Surveys do reveal that Internet users want proof that companies are utilizing security within their computer systems. Our focus should be on making security an ongoing end-to-end requirement. Senator Robert Bennett (R-Utah), chairman of the Senate's High-Tech Task Force and Special Committee on Y2K said, " The issue is not privacy. We do not want privacy on the Internet. We want security. It comes down to "I'll show you my security protections if you'll show me yours." **7**

Rather than being forced into complying with legislation, network administrators and database administrators must take best practices and security guidelines into consideration. Every company should create a privacy policy and ensure that all employees adhere to that policy. Individuals should become informed and must make decisions for themselves as to what information will be divulged and what steps to privacy they will take. Personal ethics of IT professionals will come into consideration where data privacy is questioned. This is another debate taking place within our industry, one in which many IT professionals will find themselves in hot water if a policy is not in place. People who create and administer systems that are collecting personal data must understand that ethics is vital. Providing security of data, ensuring that the data is correct,

© SANS Institute 2000 - 2005 Author retains full rights.

and being aware of business ethics is only going to enhance the success of an Internet business.

Clinton Wilder reporting in INFORMATIONWEEK for February 19, 2001 wrote, "The debate over ethical standards in business isn't new. What is new, or at least more apparent than ever, is IT's central role in some of the most important business-ethic issues of the day: privacy, the ownership of personal data, and the obligations created by extended E-business partnerships. Sacrificing ethics for short-term gain is sure to lose customers and partners in the end. Ethics is not just a matter of moral correctness—it also means business success." **8** As a result, we read the media reports of failed companies that were not diligent in systems security or could not make ethical decisions related to business concerns.

Five main reasons for private sector self-regulation has been compiled by the Citizens Against Government Waste **1**

- Privacy policies are legally enforceable, giving consumers recourse if their information is misused. Nearly 90 percent of Web sites have privacy policies, and there are many resources available to establish such policies
- Privacy seals act as a badge of honor for private sector web sites, certifying that the web sites adhere to certain minimum standards that can be enforced to ensure compliance.
- Consumer education regarding online privacy is lacking, so many companies have taken the initiative to provide consumer educational seminars and conduct extensive media campaigns on how to protect you online.
- Keeping information private can be as simple as telling one's Internet browser to disable some or all cookies. Cookie managers and blockers are already embedded in every browser on the market.
- New technologies such as the Platform for Privacy Preferences (P3P), "Crowds," Lumeria and Microsoft's Hailstorm put the consumer in charge of how personal data is distributed, and to whom.

Furthermore, there can be effective enforcement by industry itself. Already there are third-party organizations that provide an identifying seal of membership; licensing companies and organizations that meet required guidelines for monitoring, verification, complaint resolution and education for customers. This approach is favored by the Online Privacy Alliance, who believes that the best way to create public trust is for organizations to alert consumers and other individuals to the organization's practices and procedures through participation in a program that has an easy to recognize symbol or seal. **9**

Network administrators and corporations must begin to design systems with security from the start. A layered defense system must be implemented if total security is to be achieved. Demonstrating to a court of law that due diligence was practiced would include everything from implementing technologies such as firewalls, intrusion-detection tools,

© SANS Institute 2000 - 2005 Author retains full rights.

content filters, traffic analyzers, anti-virus applications, proper back-up of data and virtual private networks to having best practices for continuous risk assessment and vulnerability testing. In addition, developing and implementing corporate policies and procedures demonstrates intent for addressing privacy concerns. Obviously all aspects cannot be controlled by the IT department, but every Admin should become assertive in monitoring and securing their systems. Organizations such as SANS have identified the most common vulnerabilities of online systems. Specific recommendations for operating systems are available to the community.

Security of data must become a national priority. If our industry is to continue to lead the world with eCommerce developments, then we must be diligent and proactive with strong measures to protect computer systems and the sensitive data stored on those systems. To do so will not only ensure our business success, but also our Nation's success.

Resources for further information:

The Online Privacy Alliance provides guidelines and information to organizations interested in finding out more about " online privacy." An online brochure explaining the "five essential elements to online privacy" can help aid an organization in developing increased awareness of privacy.

See the web site www.privacyalliance.org

Consumers and Home computer users that need more information for self-protection of privacy can find guidelines at the Truste web site www.truste.org

Electronic Frontier Foundation will provide guidelines to "EFF's Top 12 Ways to Protect Your Online Privacy" at http://www.eff.org/pub/Privacy/eff_privacy_top_12.html

Internet References

1. Citizens Against Government Waste. " Keeping Big Brother from Watching You" URL: http://www.cagw.org/publications/lookinglass/pub.looking.privacy-exsumm.htm (25 May 2001)

2. Lais, Sami. " No More Secrets ". 19 Feb.2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57777,00.html (25 May 2001)

3. Truste. " How Does Online Privacy Impact Your Bottom Line? ". URL: http://www.truste.org/bus/pub_bottom.html (25 May 2001)

4. Vijayan, Jaikumar. " Premier 100: Corporate executives may need security wake-up call". 22 May 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60779,00.html

© SANS Institute 2000 - 2005 Author retains full rights.

(25 May 2001)

5. Thibodeau, Patrick. " FTC Official Faults Corporate Privacy Policies". URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60248,00.html (20 May 2001)

6. Burton, Daniel. " IRS security flaw crashes Internet privacy party." URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59540,00.html (21 May 2001)

7. Verton, Dan . " Legislators eye cybersecurity ". URL: http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO59161,00.html (22 May 2001)

8. Wilder, Clinton. " Business Ethics for IT Managers – What You Can Do ". URL: http://www.informationweek.com/837/dataethics.htm (23 May 2001)

9. Online Privacy Alliance. "Effective Enforcement of Self Regulation". URL: http://www.privacyalliance.org/resources/enforcement.shtml (22 May 2001)

© SANS Institute 2000 - 2005, Author retains full rights.