Global Information Assurance Certification Paper

Disclosure: All, Partial, or None
When is it too much or not enough?

James Walker

GSEC Practical Assignment
Version: 1.4b Option 1
01/25/2004

Abstract

There are three schools of thought on the dissemination of information related to security: full, partial, and none. It would seem that all of them have their place, whether it is in the workplace, the military, federal government, or one's personal life. There are those who believe that all information should be available, regardless of the potential cost. Others believe that only certain aspects of information should be public. Businesses maintain competitive advantages through trade secrets; what if those trade secrets are available to its competitors? If minimal to no disclosure is the philosophy of others; why admit to a problem until someone catches it? Herein are the analyses of the pros and cons of each and the potential consequences.

Introduction

Information is power, and he who controls the information controls the world. Accepting this statement as fact leads us to conclude that the real-world implementation of CIA (confidentiality, integrity, and availability) as a process is crucial. The process of CIA states: information must be kept so that confidentiality is not compromised, information maintains its integrity, and information is available to only those who have need of it. Information disclosure directly relates to CIA; that is how people perform their jobs or set customer expectations. The free flow of information allows people to perform their jobs more efficiently, whereas the lack of information may bring workflow to a complete standstill. Depending on who is releasing it, the processing of information, as full, partial, or non-disclosure can be a benefit or a bane. We will look at how laws affect information disclosure, the effects they have on the information flow of a generic business model, the concept, as well as its practical business applications.

Legal Aspects

The Federal Government has set forth guidelines which private and public industry must follow; Gramm-Leach Bliley Act, Health Insurance Portability and Accountability Act, Freedom of Information Act, the Privacy Act and the Selective Disclosure and Insider Trading regulations. *Quis custodiet ipsos custodies*, who guards the guardians; the Federal Government makes the rules but often does not follow them.

1. Gramm-Leach-Bliley Act of 1999 (GLB): "… includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions."
http://www.ftc.gov/privacy/glbact/

2. Health Insurance Portability and Accountability Act 1996 (HIPAA): "The Privacy Rule, at 45 CFR parts 160 and 164, establishes a category of health information, defined as protected health information (PHI), that a covered entity may only use or disclose to others in certain circumstances and under certain conditions."
http://privacyruleandresearch.nih.gov/privacy_boards_hipaa_privacy_rule.asp

3. Freedom of Information Act of 1967 (FoIA): "Sec. 552. Public information; agency rules, opinions, orders, records, and proceedings. "Which states that each Federal agency shall make information accessible to inquiry. Provided the information does not compromise information that the Federal Government feels should remain confidential.
http://www.nih.gov/icd/od/foia/efoia.htm

4. Privacy Act of 1974 (PA): "§ 552a. Records maintained on individuals. 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 … " The act describes the conditions by which Federal Agencies are allows to disclose information when requested by the public.
http://www.usdoj.gov/04foia/privstat.htm

5. Selective Disclosure and Insider Trading: "The Securities and Exchange Commission is adopting new rules to address three issues: the selective disclosure by issuers of material nonpublic information; when insider trading liability arises in connection with a trader's "use" or "knowing possession" of material nonpublic information; and when the breach of a family or other non-business relationship may give rise to liability under the misappropriation theory of insider trading. The rules are designed to promote the full and fair disclosure of information by issuers and to clarify and enhance existing prohibitions against insider trading."
http://www.sec.gov/rules/final/33-7881.htm

Definitions

- Full Disclosure: the act of making all details of an entity public knowledge
- Partial Disclosure: revealing that which is necessary for someone to know while taking into the fact who is doing the disclosing and their intentions
- Non-Disclosure: no information revealed

Business Models

Full disclosure/Access

A customer calls a business that has ready access to the customer's personal information. The business serves the customer in a quick and efficient manner. The satisfied customer has a positive opinion of the company and will do business with them again. This increases the company's goodwill and profits.

Partial Disclosure/Access

A customer calls a business that has access to only part of the customer's information. The business requests information that the customer feels they should already know. This takes extra time for both the business and the customer. Either the customer will accept a reduced level of service or will go elsewhere. If the business believes time is money, then reduced information accessibility means fewer customers served in a given time and a decrease in revenue may result.

No Disclosure/Access

A customer calls a business and, due to confidentiality, there is no information available. The business' ability to service customers is nearly zero. The business must enter all required data each time with customer service and efficiency dropping to nearly zero. Most companies, if so operated, would quickly go out of business.

Theoretical Applications

In the private sector, disclosure of information could mean the difference between revenue gained from a sale, and revenue lost from a lawsuit. Take the case of a used car lot. A person wants to buy a car, but has no idea that had the front end completely replaced as the result of an accident. The salesperson knows of the front-end replacement, and there is no sign on the car stating the car is being sold "As is." If the salesperson chooses not to disclose the information, discovery of the front-end replacement may result in a lawsuit claming non-disclosure of a known defect. However, if the car is sold "As is" or the salesperson discloses the front-end replacement, then should be no liability on the part of the business.

In the past, there were instances where banking information was compromised. Whether the compromise involved the bank's records or a record of its account holders; the information compromise affects the employees as well as those who have a financial stake in the business. If a bank publicly announces an information compromise, account holders may close accounts and move them elsewhere. Silence was the policy, where administrators admit nothing, not even to a fellow branch. This may help in keeping incidents out of the media; however, it does nothing to solve the inherent security problem. Today, banks form alliances with each other in order to discuss issues of information security and how best to secure themselves as a whole.

The public relies on companies and the Federal Government to assure that stock prices are accurate relative to the financial status of a company. Those who work for companies have a competitive advantage over those who merely watch from the outside due to intimate knowledge about the company. Insider trading occurs when a person with intimate company knowledge attempts to manipulate the stock price when they buy or sell stock. The Security and Exchange Commission has very strict rules regarding the disclosure of information related to the value of a stock. Employees of a company must abide by those rules or face charges of insider trading. At least once a

year, there is litigation involving insider trading with Martha Stewart being the most recent example.

Practical Applications

1. Full Disclosure

Full Disclosure is the act of making all details of an entity public knowledge. In theory, this sounds like a good idea; everyone has access to all information and can accomplish a job as efficiently as possible. While it does allow for efficient information processing, it could divulge information that is not necessary. Under scrutiny, full disclosure does not make good business sense.

Full disclosure within the Military and the Federal Government does not exist. As much as the public might want to understand the decision-making process of the government, it is not in their best interest. There are people who want to know everything there is about the way the United States wages war including tactics, armaments, and ordinance. How much information can the military reveal while still effectively doing their job and protecting our troops? There are groups within the Federal Government and the military on both sides of the disclosure discussion. One side believes that because the citizenry pays their salaries, that they should disclose everything they do. The other side believes that the government works on behalf of the citizenry and it is their job to work in their best interest; therefore, they divulge information that is safe for the public to know. This is a constant struggle amongst agencies as to how much information is too much. We shall see that private industry operates much like the government.

Private industry, just as the federal government, does not operate under the auspices of full disclosure. The very nature of the phrase, 'private industry' reflects this. Would it make sense if Pepsi or Coke revealed their secret formula to the world? What if a major hospital chain revealed its hospital pricing schemes? Businesses have trade secrets, copyrights, pricing schemes, and other marketing data that they do not want made available to the public. Though the public wants to know everything about a company, it is neither practical nor good for business.

Like businesses that keep their intimate company secrets from the public, companies specializing in information technology attempt to keep secrets from those who would reveal them. Everyday, news about a new virus, exploitable code, or tools that a script-kiddie or casual hacker uses to deface websites surfaces. How much shared information is there within hacker echelons? Once again, full disclosure is not a reality. The 'Black Hats' would not normally tarnish their reputation by giving information away to those who would squander it to deface websites or in commonplace denial of service attacks. To the casual observer, full information disclosure appears to be a desirable thing, however when viewed from inside an organization, full disclosure is not practical and

sometimes detrimental to the company. Partial information disclosure might be more appropriate in this setting.

2. Partial Disclosure

Partial disclosure is revealing that which is necessary for someone to know. We must take into account who is doing the disclosing, and what is their intention?

The closest that the military and Federal government comes to total disclosure is the - http://www.nih.gov/icd/od/foia/efoia.htm , and the *Privacy Act* (PA) of 1974 -. The *Freedom of Information Act* allows the public to find out what Federal Agencies have documented about them. The public must make a formal written request for information regarding his or her own or another person's record.

The Gulf War II gave journalists and viewers an unprecedented view of war, when the military allowed journalists to travel with the troops. In the past, the news services had to rely on photographs, correspondence, hand-drawn pictures, or film that was days old. The 24-hour news services had reporters traveling with the troops and returned real-time information. Viewers saw troops, movement, and some gun fighting in real time. Even though the reporters had live cameras, they were restricted by the military as to when, what, and where they could film. Though the viewers saw more than they had ever seen before, there were still some aspects of the war missing. The military still kept a tight rein on the information and sent reporters home if they did not comply, or disclosed information that could have jeopardized the lives of troops. As the military controls broadcast information, private businesses also attempt to control the information released about them.

Insurance companies dealing with life and health matters walk a fine line when it comes to disclosure of information. They require applicants to give information that may be considered confidential. If an applicant's record is deemed an acceptable risk, the insurance company issues a policy. If the insurance company is a HIPAA covered entity; the applicant's information must be stored in a secure manner. In the case of denial, how does an applicant learn *why* their policy was denied? The first call is usually to the insurance company. Does the insurance company know? Yes, their underwriters are the ones who made the decision, but can this information be disclosed? No! The insurance company is not a medical institution and therefore, cannot disseminate *any* medically related information, even if they are taking to the person and have positive identification. The insurance company refers the applicant to their personal physician for the answer.

What does the insurance company do with the data of a declined applicant? They destroy the paper form after it is transferred to an electronic format, but how long do they keep the digitized data? States have varying requirements as to how long the information must be kept, relating to the period of time in which an

applicant can appeal the rejection. After this, the company has no business need for retention of the information, and they must keep the data until the period of appeal is past. If the applicant decides not to appeal, then the insurance company should have a process of properly destroying information.

HIPAA caused upheaval throughout healthcare and related industries. No longer are nurses having discussions in the open with family members about a loved one and 128-bit encryption is the norm as opposed to the cutting edge. Healthcare outsourcing (transcription, nursing, etc) is closely monitored, so what happens when someone receives an email like this; "Your patient records are out in the open... so you better track that person and make him pay my dues."[1] Officials at University of California San Francisco Medical Center received this message from a Pakistani woman, Lubna Baloch. Transcription Stat, a transcription company that many hospitals in the area use, employs outside contractors who, in turn, outsourced work to overseas contractors like Lubna Baloch. The contractor did not pay her, so she took action in the only way she knew how. Transcription Stat took full responsibility for the incident, and they stated they would look into contractors and their subcontractors much more carefully in the future. Other countries do not have the same information security laws; consequently, it is difficult to prosecute an information breach. Currently, we do not know how much information goes overseas for processing, but it would be in the best interest of those who are responsible for protecting information to know.

There are many resources on the Internet for finding and disseminating knowledge about information security, ranging from anti-virus sites to forums where information security professionals gather to exchange information. Several websites discuss vulnerabilities, viruses, and patches for operating systems. Symantec (www.symantec.com) is, the self-described, "*world leader in Internet security*," disseminating information regarding viruses, vulnerabilities, and patching. The Symantec DeepSight Threat Management System analyzes threats and trends through the world and sends out alerts to those who subscribe to the *Full Disclosure* mailing list. John Schwartz, President and COO of Symantec, "called for legislation to criminalize the sharing of information and online tools that can be used by malicious hackers and virus writers."[2] This affirms Symantec's stance of only disclosing information which helps combat viruses and vulnerabilities, but not everyone saw this as a positive statement. There were cries of censorship and boycotting of Symantec's products because hackers aren't the only ones who use these tools. The writers and posters on the BugTraq mailing list also use these tools to discover and publish vulnerabilities. Would these people go to jail as well? This is an example of a well intentioned statement from a company representative "biting the hand that feeds it."

[1] David Lazarus
[2] Kim Zetter

AntiOnline's (www.antionline.com) members are security professionals and novices who come together to discuss information technology and security. They also seek to spread information and best practices, so that others can benefit from their knowledge.

> "What AntiOnline IS: AO is a worldwide community of security, network and computer professionals, students and keen amateurs who come here to learn the principles and details of computer/network security."

AntiOnline warns those who would use this site for malicious intent,

> "What AntiOnline is NOT: AO is not a place where the community's knowledge is used or passed on to others in order to carry out illegal or immoral acts."

Malicious hackers in the private sector also practice partial information disclosure. They disseminate vulnerabilities and exploits to their fellow hackers. One such case is Tubul, who sells the concept of *Invisible, Bulletproof Hosting.* Until now, hackers have always considered spammers a lower form of life, just slightly higher than script-kiddies. What is the challenge of sending out massive quantities of e-mail to those who do not want it? Lately, their opinion has changed somewhat, as engineers/hackers are teaming up with spammers to set up invisible web hosting sites. Spammers are hiding websites within domains that have very strict no spam policies. Once they are active, they begin spamming from within the site. Offending sites are usually found by doing a tracert or a WHOIS lookup, however with the huge number of computers that have Trojans running, this particular group is able to return a legitimate IP address, not necessarily the hosting company or the site itself. This process is essentially invisible, bulletproof hosting. Tubul, a member of a Polish company who is offering this service, gave a demonstration from a secret spam site *within* rackshack.net.[3]

> A traceroute to the site indicated that it was being hosted on a computer apparently using cable modem service from Comcast.
> "Fake," said Tubul.
> Indeed, when a traceroute to the site was performed moments later, it appeared to be hosted on a computer with a DSL connection from Verizon.

In this example, we see hackers using their vast resources giving limited information to another group so that both can profit. This is, of course, at the expense of compromised machines.

[3] Brian McWilliams

3. Non-Disclosure

Non-disclosure is the attempt to keep as much information as possible from the public. The Federal Government and the military are famous for the phrase, "Need to know," and in their view, the public does not have a need. The opposite sides of disclosure in the government constantly battle amongst themselves over the publics' need to know.

Microsoft Corporation is infamous for its bug-ridden code and the denial thereof. It follows that they deny the exploitable vulnerabilities in their software. One on hand we have hackers who constantly hammer away at the software to see what vulnerabilities they can find/induce, and on the other, security professionals who have to work twice as hard and fast to develop, test, and deploy patches to prevent incidents. Recently, Microsoft went on the offensive with the blaster worm and alerted security professionals to the vulnerability. Wired.com commented on an article by the Associated Press.

> "We definitely want people to apply this one," said Jeff Jones, Microsoft's senior director for trustworthy computing."Outside researchers and Microsoft's own internal reviews discovered the new flaws after the Blaster infection," he said.

The success of this disclosure will hopefully teach Microsoft that being proactive will boost their image and help secure their product after it has left Redmond.

The Federal Government and the military have similar yet different levels of the term access regarding the sensitivity of information. Just because you have the proper clearance level does not mean you have the *need to know.* The Department of Defense has a third view of secret information disclosure. Information must stay out of the hands of those who do not need to know it. However, classification is not strictly based on content. Something may be classified not due not to the information itself, but the source from where the information originated. Release of that information may have dire consequences.

In August of 1998, the North Koreans tested a Taep'o Dong-1 missile by shooting it over Japan and it landed it in the Pacific Ocean. Obviously, this caused much apprehension on the part of the Japanese and her allies, including the United States. It came out in the media that the missile did not have a warhead and never posed a threat to Japan at all. This was good news and bad news at the same time. There were *very* few people in the Korean military command who knew the missile did not have a warhead, so it was not difficult to figure out who leaked the information. Because of the leak, three people were found and executed,[4] a general in the Ruling Council of the Military, his mistress, and his aide, two of which were high-level informants. The fact that the missile had no warhead was both important and classified. However, the source of that data

[4] Lutche, Michael

was far more important than the information itself. This is an example of the Department of Defense view of information confidentiality because the sources were more important then the actual information.

Preparing for Big Bother?

In reference to the machinations of the Federal Government, do we really need to know about the 'Black ops,' which may or may not exist? Some of the more famous examples of denial:

1. Area 51: where people claimed to have seen strange aircraft, guards shoot first and ask questions later. Rumor has it the Federal Government confiscated a space observatory because it could to look down on Area 51.
2. Aliens and spacecraft that were reportedly seen at Roswell New Mexico are rumored to be housed at Area 51.
3. Skunkworks: various locations around the United States where it is rumored there are tests of new and strange technologies.

This denial caused the populace continues to propagate wild myths and rumors in attempts to get the government to confess; thus far, it has not been successful.

Pre 9/11/2001

Retired Admiral John Poindexter, of the Information Assurance Office, began work in Total Information Awareness (TIA), "…like the Stasi watched East Germans -- but using technology this time, instead of people."[5] The objective of the TIA was to find patterns of terrorism by using a huge database and complex data mining tools. The TIA was a governmental attempt, in the name of national security, to scan private records in order to trend possible terrorist activity. The TIA would do this without the knowledge or consent of individuals concerned. This immediately met with extreme resistance from every angle. Politicians, information security professionals, and even the average citizen were smart enough to realize the violation their privacy and basic civil liberties. "Critics on the left and right have called TIA an attempt to impose Big Brother on Americans."[6] As a result, the Federal Legislature did not give the TIA the funds it required to function and consequently shut down. However, the hardware still exists and the program has a new name, DARPA Terrorism Information Awareness Program. This program is directly overseen by the Department of Defense. They state that "Safeguarding the privacy and the civil liberties of Americans is a bedrock principle." (DARPA) This is to assure us that our personal information and private transactions stay personal and private.

Post 9/11/2001 and the Office of Homeland Security

[5] George Paine
[6] Ryan Singel

In October of 2001, President Bush issued an Executive Order, "Establishing the Office of Homeland Security and the Homeland Security Council." Its mission is to:

1. …shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.
2. Functions. The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

As a result, the Federal Government scrutinizes everything much more closely after September 11. 2001. This is expected if we want the United States secured. Though the random information gathering of the TIA may be gone, if there is information linking a person to Al-Queda or other terrorist organizations, that person is a fool to believe the Federal government is not watching

George Orwell showed how the Government, personified as, "Big Brother" watched over every aspect of peoples lives in his book, ***1984***. Even in the guise of protection, total information disclosure is inappropriate. How far will the Federal Government go in the future to monitor information in the name of Homeland Security that was deemed inappropriate in the past?

Conclusion

In a perfect world, if everyone had full access to the *pertinent* information relative to his or her job, business would function optimally. Unfortunately, this is not a perfect world, and often we do not have access to all the *pertinent* information that would allow for optimal business efficiency. We follow many rules and regulations to assure proper information disclosure, but non-disclosure does its best to assure no information is available. As information availability drops, the less efficient a person becomes in performing a task. The struggle continues; keep information confidential, while maintaining its integrity and denying accessibility continues. Partial disclosure appears to be an answer to the conflict. Ideally, it follows the principle of least privilege; the person only has access to what he or she needs in order to perform the job. This will allow companies to function at a moderate level and retain profitability.

Work Cited

AntiOnline. http://www.AntiOnline.com

Associated Press. "Surprise! More flaws in Windows." Quoted in wired.com. (9/10/2003). http://www.wired.com/news/technology/0,1282,60393,00.html.

Bush, President George W. Executive Order Establishing Office of Homeland Security. (10/8/2001) http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html. (1/25/2004)

DARPA. Report to Congress Regarding the Terrorism Information Awareness Program. (10/27/2003).http://www.darpa.mil/body/tia/tia_report_page.htm. (11/04/2003)

Lazarus, David. "A tough lesson on medical privacy Pakistani transcriber threatens UCSF over back pay." *San Francisco Chronicle*. (10/22/2003). http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL. (12/15/2003)

Lutche, Michael. Interview with the former Theater Special Security Officer of the United States Pacific Command, Directorate for Intelligence (J2). 12/29/2003.

McWilliams, Brian. "Cloaking Device Made for Spammers." Wired.com Magazine. (10/9/2003). http://www.wired.com/news/business/0,1367,60747-2,00.html. (10/15/2003)

Paine, George. "Who Is John Poindexter?" Warblogger.com. http://www.warblogging.com/tia/poindexter.php. (12/20/2003)

Singel, Ryan. "Funding for the TIA All but Dead." Wired.com Magazine. 7/14/2003. http://www.wired.com/news/politics/0,1283,59606,00.html. (12/28/2003).

Symantec Corporation, www.symantec.com. *Symantec Offers Webcast Highlighting Findings of Latest Internet Security Threat Report*. 10/6/2003. http://www.symantec.com/press/2003/n031006.html. (10/23/2003).

Zetter, Kim. "Just Say No to Viruses and Worms." Wired.com Magazine. 9/11/2003. http://www.wired.com/news/infostructure/0,1377,60391,00.html. (10/20/2003).