Global Information Assurance Certification Paper

Title Page:

Assessing Information Security Policies: A Language Analysis

By

Kirk P. Arnett

1.4b, Option 1, Revision 1

Submitted February 23, 2004

Assessing Information Security Policies: A Language Analysis

Abstract

A company's home page now is widely recognized as its window to the world. The security/privacy policies that emanate from this page are used to provide data to build a proposed new measure of the extent of use of security-related words within these policies. This proposed measure is referred to as the information security keyword match density (ISMD). The ISMD could be used as an indicator of security emphasis to partially satisfy external reporting requirements or as a baseline from which to draw comparisons of changes in information security emphases for a given company over time. Other possible uses of this measure and its calculation methods are to compare one company's security emphasis against its competitors, or to assess security emphases across different industries. In these roles, the ISMD should be a particularly valuable measure for those who have an interest in forming business relationships with the company or in becoming customers of the company.

From an analysis of policies from the top 100 companies of the Inc500 (http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002), the overall ISMD measure is .46, and 21 of these companies have policies with ISMDs that exceed the overall measure. But, surprisingly, only 29 percent of these fast growing private companies use their window to the world to present any kind of information security policy.

Introduction

A substantial increase in the concerns relative to information security has occurred over the past two years. Indeed this increase is appropriate as the popular press routinely publishes security breach stories, which clearly indicate that today's businesses must be more protected. Recently, a CERT Coordination Center statistic reported in CIO Magazine, predicted an 86 percent increase security breaches between 2002 and 2003 (2003b). In January 2004, Gaudin offered that security experts see "major security problems for 2004" (2004). At least two questions arise because of the rise in incidents and predictions of the future. First, how are businesses beefing up security efforts? Second, how, if at all, are information security policy statements being used to communicate and guide efforts that a business is directing toward information security?

To answer these questions, an examination of the security/privacy policies that are available from the companies' web sites is useful. This examination can be accomplished by determining which sites have such a policy. Then, the number of security-related words that appear in the company's policy can be tabulated. These security-related words are identified and tabulated by matching them against a digital list of security-related keywords that have been extracted from an authoritative publication by the U.S. Federal Trade Commission. Specifically,

the FTC page at http://www.ftc.gov/bcp/conline/edcams/infosecurity/ was used to obtain the keywords, which are shown as Appendix A.

In order to glean more information from the policies, those sites with the largest number of unique security-related word matches are identified and those sites with the largest total number of occurrences of security-related word matches are identified. In addition, the ISMD measure is established for each company for ranking and comparison purposes. The following sections describe the background and relevant literature to highlight the issues surrounding information security and policies, and the methods of data collection. Finally, the findings are presented along with limitations and pertinent recommendations.

Study Background

Like most technology innovations, the Internet has brought it share of problems along with its astounding benefits. Chief among these problems is an increased need for information security. Concerns for these problems began growing after what has been labeled the "information security baptism" (Berinato, 2003) on September 18 – one week after the September 11 attacks and the day of release of the Nimda worm. But, parallel with the increased concern over cybersecurity, the economy has experienced a dramatic increase in Internet commerce. For instance, e-commerce leader Amazon reported 24 items ordered per second and 630,000 shoppers in a single hour during its peak period over the Christmas shopping season (Weiss, 2003).

For those companies who are engaged in e-commerce business on the Web, the information security issue of Internet fraud is a major concern and cost factor. According to Verisign (2003), fraudulent transactions occur in 1.06 percent of on-line transactions as opposed to only .06 percent of conventional transactions. This reason and others have led credit card merchants to charge businesses higher premiums for online use of credit cards (Verisign, 2003). The current increase in B2C e-commerce would lead to the conclusion that customers use other methods, such as the padlock at the bottom of a secure page as an indicator of security. Or, it may be that customers, armed with zero-limit-liability credit cards, exhibit little concern over fraud. However, other issues remain that limit customer relationships. For example, CIO Magazine reported a study showing that the major reason that U.S. households have not adopted online banking is security concerns (2003a). Security concerns led convenience and privacy concerns in the CIO metric. The point is that whatever reasons customers use to gain confidence in the security of on-line activities, more security is still needed.

Policies are needed

Beyond B2C e-commerce customers, B2B e-commerce customers, face-to-face clients, potential trading or supply chain partners, investors, governmental agencies, and others may be interested in the information security efforts of

companies. Today, company security efforts are difficult to determine. But, if all companies would follow the direction of leading companies profiled in this research and provide security policy links on their home pages, then security efforts could be easily assessed. Consider, for instance, a similar point of view for corporate mission statements. As a potential partner or customer of a company, one might want to view the mission statement as a part of the criteria to help decide among competitors. The mission statement alone may not directly lead to a particular company, but might be coupled with other intelligence gathered and used in the decision-making process. The mission statement (although just written words) could provide the deciding factor. Further, the absence of a mission statement might be regarded as a weakness. This research is suggesting that public information security policies, similar to public mission statements, will benefit the company and its associates.

Policies are important for all partners in the relationship

A company with a strong publicly available security policy may benefit by
1) heading off legal disputes regarding its sincerity over securing assets,
2) lowering insurance rates because of indications of strong security, and
3) gaining additional business relationships.

In fact, some predict that 2004 will be “the year to watch for security lawsuits” (Berinato, 2004). The customers and potential partners may benefit by gaining increased confidence in a company. The security policies recommended here are general in nature and specify the intent of the company to maintain information security. As such, these policies specify management’s philosophy toward safeguarding assets and form the foundation from which other policies are built. However, these policies in no way delve into the technical methods of gaining and maintaining the security to prevent potential hackers from gaining more intelligence than they might otherwise gather. Obviously, to be effective in the roles suggested, the policies must be implemented and consistently enforced.

Policy strength should be assessed

If security policies are widely available, how might an interested party determine the strength or intensity of a policy? Since technical specifics would not be available, and security budgets would not be a part of such a policy, then some other measure beyond equipment inventories and or budget figures is needed. The ISMD is proposed is a possible solution to provide such a measure. Even though many security threats exist, little is known about an individual company's stance regarding information security threats and the strength or level of commitment of the company’s security efforts. A web-based security policy measured by a metric such as the ISMD might adequately represent a company's stance in this regard.

Government regulations are slow in coming

In September 2003, the U.S. Congress renewed its efforts to impose cybersecurity requirements on private industry. The best known of these was from the House Technology, Information Policy, Intergovernmental Relations, and Census Committee chaired by Representative Adam Putnam. “Putnam's subcommittee considered the pluses and minuses of a cybersecurity reporting requirement, similar to SEC accounting reporting requirements mandated in the Sarbanes-Oxley Act of 2002” (Gross, 2003). This kind of legislation would dictate top-level management involvement in cybersecurity issues and could require the use of a specific metric or standard. The committee’s proposal would have required all publicly traded companies including utilities and banks to conduct computer security assessment and to report the findings from the assessments to the Security and Exchange Commission (SEC). The proposal has currently been delayed because of beliefs that the SEC was not equipped to make such rules (Gross, 2003).

Only two weeks after the delay, three independent analysts, including former White House security adviser Richard Clarke, criticized the government, information technology industry, and end users for inadequate efforts to improve cybersecurity (Verton, 2003). At the same meeting, John Pescatore of the Gartner group stated that the government needed to improve its own state of cybersecurity before forcing regulations on industry (Verton, 2003). A group of information security professionals also recently formed a CSO council with a goal to foster a better partnership between business and government on cybersecurity issues (Evers, 2003).

Despite the corporate rebuff of government plans and caveats from security experts, efforts in the direction of security reporting requirements for business probably will continue. For example, committee witness Daniel Burton, vice president of security vendor Entrust, Inc., said that a report, which would be different for different companies with different risks, would allow stockholders and boards of directors to determine for themselves whether a company is adequately dealing with cybersecurity (Gross, 2003).

As widely noted, offline and online incidents provide strong evidence that business should increase security efforts. At this point, little is known about how business has responded to this need. Businesses could communicate to concerned customers and other business partners by publishing strong information security policies that are widely and easily accessible, such as web-based policies. Then policies might also satisfy a part of the reporting requirements suggested by Burton in Gross (2003) as noted above.

InfoWorld's security adviser Wayne Rash notes that most companies make a common mistake of having no security policy (2003). If businesses will develop

and publish policies that specify their intent to guard information resources and that enumerate expectations for people who access information resources, then employees, customers, and other business partners will likely become more confident. Then, the policies can be used as a springboard to help raise investor and consumer confidence that has been badly shaken by recent corporate scandals. Today, on the web, these policies are frequently embedded in the business's privacy policy because of the company's obligation to protect information that is harvested from visitors to the Web site.

So, what is an information security policy? A good starting point might be the following definitions:

> A security policy is a formal statement of rules by which people who are given access to an organization's technology and information assets must abide (Convery and Trudel, 2003).
>
> Policies are broad statements of vision that express a company's commitment to security and that lay out key values and principles that will guide corporate security activities (Panko, 2003, p. 409).
>
> A security policy goes far beyond the simple idea of keeping the bad guys out. It's a very complex document, meant to govern data access, Web-surfing habits, use of passwords or encryption, e-mail attachments, use of Java and ActiveX, and more. It should include these rules and also address physical security for individuals or groups of individuals throughout the company (Spafford, 2003).

Whereas the third example addresses specifics, the first two broad-based approaches represent the type of policy suggested by this research. Because many varieties and levels of detail for information security policies exist, publicly available resources to support their creation are needed. Fortunately, help is readily available. Books and numerous Internet sites provide templates that can be used as starting points. SANS Institute publishes a web site (http://www.sans.org/resources/policies/) to provide no-cost resources to develop and implement information security policies. This living document assists policy developers with policy start-ups in 24 security areas including acceptable use, acceptable encryption, anti-virus, ASP, email, access, ethics, Lab, password, router, server, VPN, wireless and others. SANS Institute's acceptable use area most closely represents the policies examined in this research.

No magic formula exists for every case, but a guideline for these web-based policies is worth stating. The policy should state in a convincing way the company's intent to provide a secure environment for the information assets that it holds and for Internet-based transactions that it processes. In Panko's language (2004), the policy should lay out the key values and principles as security guidelines. These guidelines would be strategic level policies used to drive lower level policies, procedures, and technologies employed in

safeguarding information resources. In some cases they would be acceptable use and information protection policies. It would make no sense to have a router access control list policy widely available, because it should remain confidential. However, a company would want to state policies regarding efforts to protect credit card and other personal information. So, the emphasis here is to access information security policies that might be subsumed in a company's privacy policy. The information assets to be protected are much greater than the personal information regarding customers, but in most cases, personal information will be a part of those assets.

Volonino and Robinson (2003) suggest that business should employ a top-down digital liability defense model (DLM) that emphasizes the need for commitment of the top members of the business. Researchers in several contexts have emphasized the importance of top level commitment as a success factor, the basis of the top level of the DLM. The second level of the DLM is statement of practice and acceptable use. Further in the model comes the notion that both technology and policy are necessary to have information security success. Documentation of policies and/or technology components of the policies might measure this approach. Or, security expenditures and their categories might be used to measure the investment in a DLM similar to the findings from the Berinino (2003) study with PriceWaterhouseCoopers, which noted that businesses are just now beginning to appreciate security as an ongoing discipline. No matter what other combination of measures might be in place for assessing security emphasis, this paper offers a non-obtrusive approach to obtain a new measure to shed light on the extent to which web-accessible information security policies address information security. The acceptable use policies and other statements of practice that show up in privacy policies are most tightly integrated with the analysis of this research.

All businesses should have a general information security policy available to the outside world. This recommendation applies to both public and private businesses. As noted earlier by Rash (2003), absence of a security policy is a mistake. Each business needs to have a policy and to make the policy evident to insiders as well as to the outside world. The analysis that follows provides a current snapshot of what is being used for information security policies that are posted on the web sites of fast growing private companies. The primary basis for comparison is the proposed ISMD.

Brief Methods

This research utilizes a partial replication of a methodology from Liu and Arnett (2002) to examine the privacy, or if available, security policies of the top 100 companies in the Inc500 http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002. This examination consists of unobtrusive methods (Webb et. al, 1966) and involves a content analysis of the available policies from web sites. The Inc500 is composed

of the fastest growing companies where growth is measured by the change in sales from 1998-2002. Eighty-four percent of the Inc500 owners started companies without any benefit of marketing research (http://www.inc.com/magazine/20031015/profiles.html).
Therefore it might be assumed that many of these owners started their companies without professional assistance regarding information security. While companies in the Inc500 are not publicly traded today, many of them will be in the future if historical patterns continue. To be eligible for the list, the company must:

> Be a U.S. owned company,
> be independent and privately held (not a subsidiary or a division),
> have had sales of at least $200,000 in 1998,
> have a five-year sales history that includes an increase in 2002 sales over 2001 sales, and
> not be a holding company.

Two options were identified for the content analysis. A text analysis program from the data mining company, Megaputer (http://www.megaputer.com) or a custom developed software application could be used. The latter was chosen because of cost concerns and because the analysis needed to be separately made for up to 100 companies rather than for a complete collection of policies of all companies. The custom-developed VBScript program used the *file system object* with the *readline* and *split* functions to 1) select each word in the policy statement, and 2) to match the word against the digital list of security-related keywords shown in Appendix A. A successful match was tabulated for each security-related word for each company along with a total word count of the policy.

To prepare the file for the analysis, each company's information security or privacy policy was copied and pasted into a single file. Two asterisks and the company name preceded each policy. If there was no policy, then only the two asterisks and company name were included. The companies are available from http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002.

The tabulation of policy words, security-related keyword matches, and the occurrences of each matched security-related keyword represent the findings of this research. An assumption is that higher levels of information security-related keyword match density (ISMD) likely imply higher levels of information security emphasis. Information security-related keyword match density is the percent of policy words that are security-related keywords. For example, words such as *security*, *virus*, and *protect* are included in the list of security-related keywords. If a single policy of one thousand words had two occurrences of the word *security*, zero occurrences of the word *virus*, and three occurrences of the word *protect*; then the ISMD would be (2+0+3) = 5/1000*100 or .5%.

The keywords were manually extracted from the "Computer Information Security Link" (http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html) of the FTC home page. These words that represent the digital list are shown in Appendix A. Applicable variations of the keywords were included to better facilitate the match. Therefore, protect, protects, protected, and protection are included in the digital list used for the match.

Findings

The policy data were collected in October 2003 and stored in a single text file on a Windows 2003 server computer. The VBScript program described in the preceding section was created to read the file and provide site-by-site counts of the number of occurrences of each matching keyword. Figure 1 from an actual "Security & Privacy Policy" of Orange Glo International illustrates the comparison. The Orange Glo security policy is located in paragraph nine of (http://www.greatcleaners.com/ogi_retail/ogi_content/shop/ogi_privacypolicy.asp)

> *We use industry-standard encryption technologies when transferring and receiving consumer data exchanged with our site. When we transfer and receive certain types of* ***sensitive*** *information such as financial information, we redirect visitors to a* ***secure*** *server and will notify visitors through a pop-up screen on our site. While we cannot ensure the* ***security*** *of Internet communications, once we receive a communication from you, we have* ***security*** *measures in place to* ***protect*** *against the loss,* ***misuse****, and alteration of any personal information that you voluntarily provide.*

Figure 1. Security Policy from Orange Glo International Policy http://www.greatcleaners.com/ogi_retail/ogi_content/shop/ogi_privacypolicy.asp

Using this security policy and matching each word against the words in Appendix A, six occurrences of security-related keywords -- those shown in bold -- would be tabulated. Five unique security-related keywords are shown in Figure 1, and the security policy consists of 85 total words.

Of the 100 companies examined from the Inc500, all but six listed a public web site. Of those 94 that listed a web site, 29 of the web sites (29 percent) contained a privacy or security policy. This finding, although web-based for only U.S. privately held companies, has similar percentages to a U.K. study reported in Volonino and Robinson (2003) where 27 percent of 1,000 companies had a documented security policy.

Overview of research tables
The tables below present interesting findings from this study. Table 1 shows the top-10 words in the policies in terms of the total number of occurrences. Table 2 shows the top-10 sites for the total number of security keyword occurrences. Table 3 shows the top-10 sites for the total number of unique security-related keywords. Table 4 presents the top-10 sites ordered by information security keyword match density (ISMD). Finally, Table 5 shows the six companies that appear in a top three listing of any of the previous tables. The Inc500 rankings and home page links are also presented in the table.

For the entire study, the web sites of 94 companies on the Inc500 list were visited. At each site efforts were made to extract the best representation of a security policy and to place the extracted text into the common file. In total, the policies had 56,511 words and 263 keyword matches for an overall information security keyword match density (ISMD) of .46 percent. Twenty-one of the sites had an ISMD greater than the overall ISMD.

Limitations of findings
The choice of an FTC model from which to select information security keywords (Refer to Appendix A) can be questioned, and it could be argued that some additional keywords should be added while others should be deleted. For instance, in the Orange Glo policy shown as Fig. 1, "encryption" and "ensure" are obviously intended to reference a facet of security practice for the company, but these keywords are not included in the appendix. In addition, a security keyword could be used in a different context, but still be tabulated to count as a security keyword. For example, the word "security" in the following sentence would be interpreted as a security keyword.

*Our company has no **security** policy.*

In addition to the keyword in context problem illustrated above, problems could arise with the total amount of the policy (total number of words) that were cut and pasted to the text file. Efforts were undertaken to make the cut and paste operations consistent among sites, but the extent of the privacy policies devoted to security differs greatly. Also, it might be argued that companies who do not directly take orders from their web sites should not be expected to address information security. But consider that many of these sites accept inquiries, employment applications, medical information, etc., and others use technologies to capture IP addresses, browser types, etc. Therefore, there is a strong possibility that personal information could be collected, or that some a site visitor tracking mechanism might be in place. Further, these companies are using the web to communicate company culture to potential business partners. Because of these reasons, all companies that intend to operate a business should have a

publicly available security policy. A minor limitation of this study is that the current Inc500 listing at http://www.inc.com/inc500/ was published after the data for this study was collected in October 2003. Therefore, the companies in this research will be different than those from the current Inc500 rankings. However, this problem is widely recognized as being present in all studies of the dynamic business environment.

Results of Findings

Obviously, the security-related keyword "security" topped the list of number of occurrences (see Table 1). In fact, this one word had more occurrences than the bottom seven keywords combined. Although far fewer occurrences than "security," the second and third ranked keywords "secure" and "protect" each had more than 40 occurrences in the policies that were examined.

Table 1 – Number of Security-Related Keyword Occurrences
Source: Web-based policies of Inc companies from
http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002&schCompany=&schKeyword=&schState=

Security	75
Secure	47
Protect	45
Password	15
Risk	13
Prevent	11
Safeguard	10
Safety	9
Proprietary	9
Critical	4

Note: Only 29 of the top 100 companies have a policy.

Table 2 provides a list of the companies that have the most occurrences of security-related keywords mentioned in their policies. Connected, Hat World, and Greenwich Technologies all have more than 20 occurrences of security-related keywords. Refer to Table 5 for a link to the home page of each company in the top three ranks in the tables. These companies represent computer software, apparel, and IT consulting respectively. For instance, Connected is the leading provider of storage software for automated protection, archiving and recovery of distributed data (http://www.connected.com/solution/index.asp). Security is the very nature of Connected's business model. Greenwich Technologies applies consulting skills to technologies including systems and storage, internetworking, application and network performance management, security, and voice/data convergence (http://www.greenwichtech.com/Content.aspx?wTR66ByP4fY). Security consulting is a core business activity of Greenwich Technologies; therefore, it is crucial for the company to demonstrate security leadership. A high

level of security emphasis is extremely important for these two companies engaged in security-related businesses. Perhaps the surprise in the rankings is the large number of security-related keywords used in the Hat World policy. Hat World claims to be the undisputed athletic specialty headwear leader with more than 400 stores selling college and professional branded headwear (http://www.hatworld.com/about_us.html). Customers can conduct e-commerce shopping-cart activities with Hat World which collects personal and credit card information. Therefore, Hat World has a need to exercise strong security and another need to inform customers about its information security policy.

Additionally, both Greenwich and Connected appear in the top three ranked companies in Table 3. Hat World holds the number four place in this ranked listing of unique security-related keywords. The maximum number of keywords in a policy is 10 (Speakeasy), which is closely followed by Connected, Greenwich Technologies, and Hat World. Comparison of the companies with high rankings of total number of keyword occurrences in Table 2 with those companies who have high rankings of unique keyword occurrences in Table 3 shows that companies typically repeat several security-related keywords in their policies.

Table 2 Companies with Largest Number of Keywords Occurrences
Source: Web-based policies of Inc companies from
http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002&schCompany=&schKeyword=&schState=

Connected	24
Hat World	24
Greenwich Technologies	23
Speakeasy	19
CoAdvantage Resources	15
Promethesus Labs	14
Orange Glo	10
NLX	10
Virtual	10
Scooter Store	8

As noted in Table 3, Speakeasy is the leader of the companies with the largest number of unique keywords and is also a newcomer to a top three listing for any of the tables. According to the web site, “Speakeasy, with broadband as its core focus, has grown into the nation's largest independent broadband service provider” (http://www.speakeasy.net/main.php?page=pr091503). The ISP orientation of this business dictates need for high levels of emphasis on computer security. An ISP company could not long survive without a strong security emphasis, because of the effect that absence of security efforts would have on customer perceptions.

Table 3 Companies with Largest Number of Unique Keywords
Source: Web-based policies of Inc companies from
http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002&schCompany=&schKeyword=&schState=

Speakeasy	10
Connected	9
Greenwich Technologies	8
Hat World	7
CoAdvantage Resources	6
Promethesus Labs	5
NLX	5
Investment	5
Scooter Store	4
Advanced Internet	4
Tastefully Simple	4
Telesynthesis	4

The findings in Table 4 present the new measurement created in this study -- the use of the index (ISMD) to rank companies as to the strength of their security policy. According to this study, Greenwich, which ranked number 9 in the 2002 Inc500 growth listing, represents a company with a security intensive policy. This is not surprising as Greenwich states that it has the technological expertise to "apply best practice consulting skills" to business technologies, including Internetworking, etc. The Outsource group ranked number 1 in the Inc500 listing. As its name implies, The Outsource Group (TOG) specializes in providing outsourcing services to its clients (http://www.tog-usa.com/index.html?Id=2262). TOG's specialty is handling the accounts receivable of its clients. Therefore, financial transactions and information that must remain secure are processed by TOG. The second place ISMD ranking provides evidence of the security emphasis of TOG. Heartland Payment Systems, the third company in the ISMD rankings and number 57 in the 2002 Inc500 rankings, provides credit and debit card payroll processing services to its client companies (http://www.heartlandpaymentsystems.com/). Clearly, payroll processing dictates a high need for information security, and Heartland's ranking on the ISMD list is no surprise. Finally, it is worth note that the top two ISMD companies also are in the top 10 ranking from the Inc500 growth list. Could this mean that highly successful private companies are highly concerned about information security?

Table 4 Information Security Keyword Match Density (ISMD)
Source: Web-based policies of Inc companies from
http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002&schCompany=&schKeyword=&schState=

Greenwich Technologies	1.69
The Outsource Group	1.68
Heartland	1.40
NLX	1.20
CoAdvantage	1.14
TripWire	1.06
Hat World	0.90
Orange Glo	0.78
Invision	0.77
Scooter Store	0.67
Sterling Financial	0.64
Synergy	0.64

The companies that ranked in the top three spots of security-related keyword intensity in Tables 2-4 above are shown in Table 5. Because some of the companies appear in more than one top-three ranking in the tables, only six companies are shown in Table 5. An interesting point of this table is the relationship in the rankings between the Inc500 criteria (based on revenue growth), and the ISMD criteria, which is based on security-related keyword matches. All but one of the top-three ranked companies from the Tables is in the top-half of the 100 companies that were selected from the Inc500 for the study. Heartland, the company that is not in the top-half is very near the top-half with a number 57 ranking. Further note that two of the companies (The Outsource Group, and Greenwich Technologies) are in the top-10 ranking from the Inc500 (http://www.inc.com/apps/inc500/searchResults.jsp?schYear=2002&schCompany=&schKeyword=&schState=). Additionally, the number nine Inc500 ranked company, Greenwich, appears in the top-three rank of tables 2, 3, and 4. Although speculative, this may imply that high growth performance companies are more in tune with the need for high levels of information security, and thus have security policies that are rich in security-related keywords.

Table 5 - Inc. Companies that Rank First, Second, or Third in Tables 2-4.

Company Name	**Inc Rank**	**Home Page Link**
Connected	45	http://www.connected.com/
Greenwich Technology Partners	47	http://www.greenwichtech.com/home.aspx
Hat World	50	http://www.hatworld.com/
Heartland Payment Systems	57	http://www.e-hps.com/
Outsource Group	1	http://www.tog-usa.com/
Speakeasy	47	http://www.speakeasy.net/

Conclusion

One surprise for this study is that not many of the top 100 companies in the Inc500 report address security (or privacy) from their web site home pages or its links. Disappointingly, only 29 percent have such web-based policies. This situation should change. Although the extent to which these types of policies are used in the most popular e-commerce oriented web sites is not known, expectations are that it would be much higher. Similarly, these percentages are expected to be considerably higher for large, publicly-held companies in the Fortune500 listings. The ISMD that was developed in this research serves as a baseline for the fast growing private companies of the Inc500. Because of their demonstrated growth to date, these companies can be expected to be the commerce leaders of tomorrow. In that role, they must better address these security concerns. Eventually, government pressure for businesses to better address security will come, but for the time being, businesses should take a more proactive role. This proactive role could pay dividends in terms of employee, customer, and investor confidence gains that may occur. If the policies are successfully implemented, other dividends may surface in terms of lower insurance rates and protection against lawsuits. Policies of the companies in Table 4 with high levels of ISMD would be good models to use when more companies begin to address security from their web windows to the world. The ISMD is an imperfect measure, but it is a start for a method to externally determine the extent of security emphasis in a company.

Appendix A – Security Keywords
Source: http://www.ftc.gov/bcp/conline/edcams/infosecurity/

anti-virus
backup
child-predator
compromise
contingency
continuity
crime
critical
disaster
firewall
flood
hacker
infect
misuse
password
pornography
precaution
predator
prevent
proprietary
protect
recover
risk
safeguard
safe
safety
secure
security
sensitive
steal
virus
worm

Works Cited

Berinato, Scott. “The state of information security 2003.” *CIO Magazine*. 15 Oct. 2003. <http://www.cio.com/archive/101503/state.html>.

Berinato, Scott. “Courts make users liable for security glitches.” *CIO Magazine*. 1 Feb. 2004. <http://www.cio.com/archive/020104/tl_litigation.html>.

“Computer information security.” *Federal Trade Commission*, 31 Aug. 2003. <http://www.ftc.gov/bcp/conline/edcams/infosecurity>.

Connected Home Page. <http://www.connected.com/>.

Convery, Sean and Bernie Trudel. “SAFE: A security blueprint for enterprise networks.” *Cisco Systems White Paper*. Copyright 1992-2003, p. 64.

Evers, Joris. “Update: Security professionals form CSO council.” *ComputerWorld*. 12 Nov. 2003. <http://www.computerworld.com/printthis/2003/0,4814,87066,00.html>.

Gaudin, Sharon. “Last year’s security problems may balloon in 2004.” *CIO Magazine*. 14 Jan. 2003. <http://itmanagement.earthweb.com/secu/article.php/3299121>.

Greenwich Technology Partners Home Page. <http://www.greenwichtech.com/home.aspx>.

Gross, Grant. “Next: Laws to guard cyberspace?” *PC World*. 4 Sept. 2003. <http://www.pcworld.com/news/article/0,aid,112330,00.asp>.

Hat World Home Page. <http://www.hatworld.com/>.

Heartland Payment Systems Home Page. <http://www.e-hps.com/>.

Inc. Home Page. <http://www.inc.com>.

Liu, Chang and K.P. Arnett. “Raising a red flag on global WWW privacy policies.” *The Journal of Computer Information Systems* 43.1 (2002): 117-127.

Outsource Group Home Page. <http://www.tog-usa.com/>.

Panko, R.R. *Corporate Computer and Network Security.* Upper Saddle River, NJ: Pearson Prentice Hall, 2004.

Rash, Wayne. “Basic security is the best foundation.” Subscriber’s e-mail. 18 Dec. 2003. *InfoWorld*.

“The SANS security policy project.” SANS Institute: Michele Guel, Project Director. 11 Nov. 2003. <http://www.sans.org/resources/policies/>.

2003a. “Security concerns prevent on-line banking for some.” *CIO Magazine*. 13 June 2003. <http://www2.cio.com/metrics/2003/metric559.html?CATEGORY=29&NAME=Security%20&%20Privacy>.

Spafford, George. "Taking Policies from useless to useful." 11 Nov. 2003. <http://itmanagement.earthweb.com/netsys/article.php/3107331>.

Speakeasy Home Page. <http://www.speakeasy.net/>.

2003b. “2003 Security Incident Tally at 76,404.” *CIO Magazine*. 31 July 2003. <http://www2.cio.com/metrics/2003/metric584.html?CATEGORY=29&NAME=Security%20&%20Privacy>.

Volonino, L and Stephen R. Robinson. *Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004.

Verton, Dan. "Cybersecurity debate heats up." *ComputerWorld*. 12 Dec. 2003. <http://www.computerworld.com/printthis/2003/0,4814,88180,00.html>.

Webb, E.J., D.T. Campbell, R.D. Schwartz, and L. Sechrest. *Unobtrusive measures: Nonreactive research in the social sciences*. Chicago, IL: Rand McNally & Company, 1966.

Weiss, Todd R. “Busiest holiday season yet for Amazon.com.” *ComputerWorld*. 26 Dec. 2003. <http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,88584,00.html>.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event