symantec™

Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals

By Sarah Gordon
Senior Research Fellow
Symantec Security Response

INSIDE

INSIDE

Contents

Abstract

As technology continues to modify the ways in which information of all types is stored, analyzed and exchanged, concerns related to privacy are growing. At the same time, the very concept of privacy is highly subjective, varying culturally as well as organizationally. In this presentation some of the cultural and organizational aspects of privacy will be examined, and some Internet-related threats to privacy discussed. Then, new survey data from our study of user behavior and technical facilitators of privacy will be presented. The study focuses on users' attitudes toward privacy and their responses to some globally applicable privacy-related threats. The data show some unexpected results, which will be interpreted by application of several well-known psychological models to the user behavior. Finally, the need for further work in the field is highlighted, and suggestions for further research provided.

What is Privacy?

Privacy is a relatively new concept. While the word "privacy" first appeared in the 15th century, the meaning most closely related to how the word is used today did not emerge for another four hundred years. As shown by the following varied views of privacy, privacy is comprised conceptually of both private and public spaces; it is context dependent and varies from person to person.

For some, privacy is exercising control over the information about themselves, or their family, that others have access to [Chess, 2003; Stefnisson, 2003]. For others, privacy is only doing things that have been expressly permitted with personal information [Whalley, 2003]. Privacy is sometimes seen as extending from information about a person to information about what a person does: for example, [Raiu, 2003] states "privacy is all data I'm working with and which shouldn't be available to just anyone is part of my (personal) privacy, and that includes e-mails, malware collections, or program sources." Some believe privacy consists of preventing others from knowing things which they know, but do not wish them to know; thus, it could be related to any type of information - not just information about oneself [Shipp, 2003]. For some, privacy extends to a right to prevent being contacted or approached by parties without consent [Kaminsky, 2003]; many people's perspective on UCE (Unsolicited Commercial Email, or Spam) illustrates this view of privacy.

In terms of popular usage, dictionaries tend to provide an excellent insight into the way a word is commonly used [Websters, 2003] defines privacy as "the quality or state of being apart from company or observation; freedom from unauthorized intrusion," and does not specify whether this relates to people or data. [OED, 2003] states privacy is "The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion." Given these varied definitions of privacy, it is important to define the aspect of privacy that this study attempts to investigate. Based upon the explosion of Internet access, it seems meaningful for the purpose of this paper to operationally define privacy as the control over the disclosure of information about one's self or personal transactions.

Culture, Gender and Privacy

The concept of privacy is ever evolving; today individuals face a wide variety of privacy concerns. One of these concerns is how companies or organizations handle private, or personal, information provided by the individual. There are some cultural differences in the amount of trust we put in others to handle this type of personal information. For example, a 1999 study by [IBM, 1999] found that Americans slightly placed more confidence in companies handling of their personal information than did people from Germany or the United Kingdom. However, there are also differences in how we perceive what information should be publicly available in the first place. In Sweden, for example, some information from tax returns is public information, whereas in some other countries, this would be considered a gross violation of privacy "rights"[1]. Many other cultural differences in privacy exist. For example, homes in Arabian society are constructed so that the residents of the house cannot see their neighbors from any part of the house, thus insuring the privacy of the neighbors [Al-Sabt, 1995]. Interestingly, this cultural expectation for privacy of one's neighbors rests primarily not upon the neighbors, but upon the one building the house that might allow for inadvertent viewing of the neighbors. [Fullbright, 2003] comments on Japanese privacy norms: "Americans frequently comment on the different sense of privacy, both physical and psychological, between Japanese and Americans…. In the bank when conducting a transaction or using the cash machine, it may be disconcerting to find someone standing right behind you … in the typical hospital or dentist's office the doctor will examine the patient not in an enclosed private office but frequently in a curtained-off area."

Gender also appears to play a role in some of the issues related to privacy. Many, if not most, studies on gender and privacy have focused on behaviors that sexually objectify women such as the use of skirt-cams, pretexting, familial abuse and societally imposed modesty [Allen, 2000; Marx, 2003]. A recent study by Information Technology Association of America found that women felt half as safe as men online, in several areas including the control over disclosure of their private information [ITAA, 2003]. One thing is clear from the existing research: women and men differ in what they believe about privacy, what they expect in terms of privacy, and in what they are willing to do to protect their privacy.

[1] While in the U.S, the Freedom of Information (1966) and Canada's Privacy Act (1985) were both established relatively recently, Sweden's Freedom of the Press laws were established in the early 1700s, and set a precedent for conceptualizing "private information".

Technical Aspects of Privacy

Aside from the different cultural expectations and definitions of privacy, one of the reasons why the concept of privacy has become so important is the ability of technology to provide for massive and fundamental changes in terms of abuses of privacy. As a trivial example, consider the "contemporary" issues of privacy from 100 or even 50 years ago. Many transactions were carried out in cash, essentially making them untraceable. Public records, if they existed at all, had to be manually searched. The process of inference (determining classified information from a large number of unclassified records) was difficult and time-consuming.

A quick comparison to the interconnected world of today provides an astonishing contrast. While we have always offered up personal information about ourselves (for example, when applying for insurance or benefits, obtaining medical services, filing tax returns, applying for employment, seeking credit, getting a mortgage, etc.), this information was relatively secure. However, the advent of large databases maintained by companies that specialize in collecting huge numbers of public records allows for the trivial monitoring and investigation of an individual. Data mining makes the process of inference cheap and easy, and the move from cash to credit cards, phones to cellular phones and paper mail to email make the task of investigating a particular citizen easier.

Although many facets of the impact technology can have on privacy are well explored by experts in law and public policy, there are some gaps in research to date. As we examine some of the previously unexplored issues, we will first consider inadvertent disclosure of private information - the "leakage" of information that the user either explicitly or implicitly allows whilst using his computer. Following this, we will explore malicious disclosure of information, via various forms of malicious code.

Inadvertent Disclosure

There are many different ways in which a user can inadvertently compromise their privacy. For example, even the simple actions of browsing the web, downloading software or purchasing software online can impact user privacy. In this section, some of these disclosures are examined, in order to illustrate the types of risk faced.

WEB USAGE – COOKIES

A cookie is a small "blob" of data stored on the client machine during web browsing in order to maintain state [Kristol, 1997]. Cookies can be temporary (that is, they are destroyed when the browser session exits) or they can be permanent – that is, they persist for a specified unit of time, possibly indefinitely. Cookies are not universally negative – they are a necessary part of working with the WWW. However, cookies can be used to profile a particular user or computer across multiple web sites. This problem is far from new [Mayer, 1997], but seems to be increasing both in prominence and application as users become more aware of the issues.

WEB USAGE – PRIVACY POLICIES

One serious issue regarding use of the World Wide Web is that a user will often voluntarily disclose information about himself assuming that that information will not compromise his privacy. Users type personal information into a competition or survey without reading the electronic small print – that is, the print that tells them that their data submission is often sold to third parties for the undisclosed or vague purposes. Similarly, some legitimate e-commerce transactions are not 100% benign. Several well-known web sites enhance revenues by selling private information (such as name and address, buying profile, and email address). This fact is disclosed on publicly available Web site privacy policies.

EMAIL – SPAM TRACKING PIXELS

The advent of HTML-enabled email has caused several issues for those concerned with privacy. In certain popular email clients (such as Outlook), emails can be previewed in a preview pane. In the case of an HTML email, however, this preview can show whether the email was opened, indicating to the sender that the email address is "live." Some spammers will attempt to send email to "predictable" email addresses at domains and use tracking pixels to ascertain opens. These addresses of these "opened" emails are deemed more valuable; in essence, the spammer knows a live address has been found and that the message was read.

DOWNLOADS – END USER LICENSE AGREEMENTS

Another extremely serious issue for users is that of the End User License Agreement (EULA). When downloading software from the Internet, users often do not read the EULA. However, the EULA can contain information that is vital for interpreting the impact of the information provided upon the privacy of the user. Additionally, there are several examples of Adware (software that displays ads on the user's machine randomly, or that target ads based upon user profile) that is "piggybacked" with other, useful applications. One controversial piece of adware – and certainly one of the most well known – is the Gator Advertising Information Network (GAIN). This software provides several useful functions – and also can gather information about surfing habits etc. Gator is given as an example, however, because the EULA and privacy policy are exemplary; anyone running the current version Gator has, at some point, been given the opportunity to read the EULA and privacy policy, in which the functionality of the software is clearly described. Thus, the software discloses its behavior and operates with the users permission, yet some users complain vehemently about the software once they become aware of its operation and perceived impact on privacy.

Malicious Disclosure

As we have seen above, there are many cases of inadvertent information disclosure that are not in line with the traditional concept of malicious in nature. However, sometimes there is another avenue through which privacy is compromised: intentionally forced disclosure facilitated by Malicious Code. The current status of the Internet provides the perfect environment for Malicious Code; self-replicating code can take advantage of the high degree of homogeneity and interconnectivity of the Internet, and Trojan Horses can be easily and rapidly disseminated via the network. Furthermore, the blurred lines between data and code further increase the opportunity for the execution of rogue code.

PASSWORD-STEALING TROJANS

The concept behind a password-stealing Trojan is far from new: the idea of using a "trojanized" piece of software to grab passwords as they fly by, either directly from the keyboard or in transit over the network has been implemented many times on a raft of different platforms. There are currently many different password-stealing Trojans deployed on unsuspecting users' machines.

SPYWARE

As the Internet develops, the value of gathering data on groups of users and individual users behavior for commercial purposes increases. Thus, there is a legitimate desire for online marketers and web site creators to tailor content and offers to users for the purposes of cross-selling and up-selling, as well as lead generation. However, unlike its legitimate cousin, Adware, Spyware does not request permission from the user prior to installation; thus, a computer can silently track personally-identifiable information, and use this to modify content.

REMOTE ACCESS TROJANS

A Remote Access Trojan is a computer program that lets a user (or users) access machine resources remotely. Here, as is often the case when considering non-viral malware, the classification of such programs as Trojans depends significantly upon one's point of view: the tool in the hands of an administrator could be a useful method of remote management. In the hands of a hacker the same tool, silently allowing an intruder into one's machine, is certainly a Trojan Horse. A good example of this dilemma is the Cult of the Dead Cow's Back Orifice. This tool is a powerful and unobtrusive architecture for remote management… yet many users consider it to be a Trojan Horse. While the position is arguable (for a counterpoint, see [CDC, 2003]), from the perspective of a user who has had BO2K installed without his permission on his machine, it certainly fulfills the requirements of a Trojan Horse.

COMPUTER VIRUSES

Previously, the primary danger of computer viruses was data modification or destruction. However, with email now commonplace on the desktop, and connectivity readily available via a standard set of system calls, the ability for viruses to export confidential data is becoming problematic. For example [Symantec, 2002], to conform with APA style.

BLENDED THREATS

Blended threats combine the characteristics of viruses, worms, Trojan Horses, and Malicious Code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage; just as in the case of viruses, such damage is not limited to simple damage, but can involve the dissemination of private information or the installation of other threats to privacy such as Remote Access Trojans or Password-stealing Trojans.

Technical Responses to Privacy Threats

Perhaps one of the most interesting aspects of the problems outlined above is that in each case, significant reduction of risk can be achieved by modification of user behavior. In the case of inadvertent compromise, a higher awareness and more active participation in control of user information can reduce disclosure, or at least control it.

In terms of browsing the Internet, there are many controls and configuration settings with web browsers that help facilitate privacy. For example, the Platform for Privacy Preferences Project, P3P) developed by the World Wide Web Consortium (W3C) provides for the creation for machine-readable privacy policies [Marchiori, 2002]. Such policies can be read by browsers, and acted upon accordingly. Microsoft's Internet Explorer 6.0 has added support for P3P policies for cookie control, allowing cookies to be accepted or rejected based upon the user's privacy preferences [Microsoft, 2001]. Software exists which can be configured to periodically delete unwanted cookies. However, user understanding and web site support for P3P is currently sketchy at best.

Poor acceptance of technologies addressing privacy concerns is a serious problem for those tasked with maintaining large numbers of computers, and enforcing departmental or corporate policies (see survey data below). Fortunately, there are technological solutions available that allow policy to be enforced company-wide; for example, Symantec's Enterprise Security Manager is capable of enforcing rule sets for large numbers of computers automatically. Despite this technological salve, it seems that there is a significant disconnect between expressed concern and action; even informed users seem to express concern but do not follow up with actions. Similarly, protection from unwanted but legitimate software functionality is provided by inspecting most EULAs and Privacy Policies – extension of P3P to create machine-readable EULAs and policies would help automate users privacy concerns. However, until such a system is produced, reading the EULA should provide sufficient protection.

In terms of malicious privacy compromise, the solution set is yet clearer: anti-virus software protects users from the vast majority of threats. For those concerned about spyware threat mitigation is available to the user…if they choose to apply it. This point, however, is the crux of the matter, and the primary driver behind this research: do people care about their privacy, and if so, how is this reflected (or not) in their actions.

Study Goals

As outlined above, there exist many different threats to user privacy online, ranging from tracking user actions to completely taking over their machines. However, in each case the main concern is related to user behavior not technology: often a robust technological solution exists, but the crucial element is user comprehension and action.

The goal of this study, therefore, was to determine if there was consistency between a stated desire for privacy and the day-to-day actions of information security professionals related to privacy-enhancing behaviors. The hypothesis is that security practitioners believe privacy is important and they consistently practice behaviors that are consistent with their beliefs. The null hypothesis is that security practitioners believe privacy is important but their actions are not reconciled with their beliefs. If this null hypothesis is true, then the privacy they say they believe is of value is at risk. These risks are facilitated by, but are not limited to, the behaviors measured in the study.

Methodology

The preliminary design of the survey involved querying a focus group of 67 individuals working in the computer security field. In order to measure whether or not the participants valued "privacy," and to ascertain their behaviors related to certain aspects of privacy, the subjects were asked eight True/False questions related to familiarity with Personal Privacy Policy (P3P) and reading of privacy policies (their own organization, and that of sites they visited). In order to lessen possible bias with subjects determining the questions were specifically related to privacy, the question designed to assess their attitude toward the study's operational definition of privacy was placed as the 8th question, at the end of survey.

In initial findings, it was observed that no subjects expressed a familiarity with P3P; however, when queried directly using the words "personal privacy policy," a few expressed some familiarity. Thus, the survey was revised such that it was administered using the words "personal privacy policy" rather than the acronym "P3P." Several other issues were then added to measure compliance with other privacy-enhancing behaviors, such as encrypting sensitive e-mails and deleting unwanted cookies.

The final revised survey consisted of eight True/False questions designed to measure two things: six functional/operational behaviors and the subject's desire to control of information about self and transaction. It was administered to randomly selected subjects from attendees at three IT/Security Conferences held in the United States, The United Kingdom and the EU.

Responses Summary

The responses gathered in terms of True/False answers are shown in the following table, keyed by the response of the primary question concerning privacy. This was:

I like to control the disclosure of information about myself and/or my transactions.

In the US study, there were a total of 63 respondents; the UK study contained 58; the EU study contained 23. Note that despite the small number of responses in the EU study is still statistically meaningful, given that the respondent number represented over 90% of the target group. The data collected is shown below.

Question	Group	US True	US False	UK True	UK False	EU True	EU False
I am familiar with my browser P3P	Important	27	36	30	28	17	6
	Unimportant	2	6	2	0	0	0
I always encrypt sensitive email messages	Important	26	37	21	37	8	15
	Unimportant	4	4	1	1	0	0
I encrypt all emails	Important	0	63	3	55	0	23
	Unimportant	0	8	0	2	0	0
I always delete cookies I do not need	Important	39	24	30	28	13	10
	Unimportant	2	6	1	1	0	0
I always read the privacy policy of web sites I visit	Important	3	60	11	47	4	19
	Unimportant	0	8	1	1	0	0
I always read the entire EULA of new software before agreeing to install it on my computer	Important	10	53	5	53	1	22
	Unimportant	2	6	0	2	0	0
I always encrypt data on my hard disk	Important	10	53	10	48	1	22
	Unimportant	0	8	1	1	0	0

Table 1: *Aggregate data from the study for US, UK and EU audiences. Note the large disparity between concern about privacy and actual behavior.*

Analysis

Analysis of the data is fairly straightforward, as the results are incredibly clear: even a "by eye" analysis shows that there is a huge disconnect between belief and action. In the case of each country set, the vast majority of users expressed concern over personal information disclosure. However, the actions taken (or more frequently) not taken show a massive disregard for these concerns.

It is not possible to attribute this disconnect to technological naiveté. Consider the question regarding web site privacy policies. In this case, the US data shows that of the 63 users who expressed that they valued privacy, only three always read privacy policies on Web sites. Similarly, on the question regarding End User License Agreements, only 10 users claimed to reliably read the policy. The data from the UK and EU studies show similar behavioral biases. Given the user demographics (those people attending a security conference or trade show) it is difficult to argue that users were ignorant of the dangers inherent in installing and running executable code, yet the overwhelming majority of users did not even perform the rudimentary step of checking the claims of the software supplier.

Even in cases where there is a good and free technology solution available, such as P3P, our initial data showed that while users claimed that they were aware of the technology, further questioning revealed that there was a very low understanding of this technology. While approximately 50% of respondents stated they were familiar, conversational evidence clearly indicated that this number was higher than the real statistics. Thus, many users are actually unaware of the free and embedded technology solutions available to them.

Cognition

Given the rather surprising nature of the results and the large disconnect between belief and response, it behooves us to discuss the underlying mechanism for this situation. Although further research is indicated, it appears unlikely that unwieldiness of technical solutions can be entirely blamed for the observed data. Even in cases where technology has been introduced to safeguard user privacy, there seems to be an apathy regarding its use or even understanding.

One model for representing contradictory cognitions is the cognitive dissonance model [Festinger 1957]. This model applies when one holds two competing thoughts or actions. For example, imagine someone has just purchased a new cellular telephone phone with free WWW access, and signed a two-year service contract[2]. The next day, a new offer arrives - upgraded phone (i.e. camera phone), and free service for six months, with no contract. The person now has two competing thoughts: the belief that they signed up for a good deal, contrasted with new parameters that are, on the surface, more attractive.

The conflict, or dissonance, could be resolved in a number of different ways. The buyer could focus on the good things they got in their deal – the strengths of the offer they accepted (i.e. free WWW access, stability of two-year with no price change, etc.). They may focus on the fact it was the "right time" to make such a purchase. At the same time, they may diminish the value of the competing belief by dismissing the extra functionality (camera) as superfluous. The amount of dissonance is affected by two factors: the number of beliefs in conflict, and the importance, or strength, of those beliefs[3].

The data gathered in this current study indicate the presence of some type of dissonance between the desire to control disclosure and the thinking regarding the actual behaviors engaged in. This process certainly threatens the privacy of users, and, as most of the individuals involved in the study were decision makers or actors in the security process, has the potential for a more widespread impact. Future research will examine ways in which dissonance can be resolved in which help, rather than harm, organizational security.

Conclusion

The results of this study provide interesting food for thought. Despite the fact that there exist many impediments to online privacy and that educated users expressed a strong concern for their privacy, the behaviors claimed by respondents do not reflect these concerns. This result is of little surprise to the security consultant, but may be of some surprise to industry observers: there is a disconnection between the risk and the behavior.

The significance of this result for future work is clear: more research should be done to understand why the behavior does not match the concern regarding privacy. As discussed above, when the human mind encounters data that is inconsistent with behavior this dissonance must be resolved. By understanding the ways in which users are currently resolving this dissonance while continuing to engage in "at risk" behaviors, education and product design can be modified such that the risk is mitigated most effectively. The weakest link in the computer security chain remains the person using the computer: research that emphasizes strengthening this crucial link will provide the largest increase of security and the best possible research benefit.

[2] People tend avoid input that will increase dissonance; however, sometimes the beliefs are forced upon them.
[3] One seemingly contradictory result noted by Festinger was that when a person acts against their internal beliefs, the smaller the reward for doing so, the larger the generated dissonance. In a classic experiment [Festinger & Carlsmith, 1959], Festinger "rewarded" participants for espousing a position that they did not actually believe. Interestingly, those who were rewarded least showed the greatest shift in their own personal belief system.

References

Al-Sabt. M. 1995. Arabian Business and Cultural Guide. Published by Traderscity.com.

Allen, A. 2000. Women, Privacy and Cyberspace, Stanford University Symposium on "Cyberspace and Privacy: A New Legal Paradigm".

CDC. 2003. Cult of the Dead Cow, A Note on Product Legitimacy and Security, available online at http://www.bo2k.com/docs/bo2k_legitimacy.html

Chess, D. 2003. Personal correspondence. Used with permission.

Festinger, L. 1957. Theory of Cognitive Dissonance. Stanford University Press. Stanford, CA:

Festinger, L. & Carlsmith, J. 1959. Cognitive Consequences of Forced Compliance. Journal of Abnormal and Social Psychology, 58, pp. 203-210.

Fullbright. 2003. Retrieved from the World Wide Web July 1, 2003. http://www.fulbright.jp/e4/ayjcont4.html.

IBM Corporation. 1999. IBM Multi-National Consumer Privacy Study. IBM Global Services. IBM Corporation. Yorktown Heights, NY.

ITAA. 2003. Security and Privacy National Attitudes Research Study. Retrieved from the World Wide Web on July 15, 2003. http://www.itaa.org/infosec/faith.pdf

Kaminsky, J. 2003. Personal Correspondence. Used with permission.

Kristol D. & Montulli L. 1997. HTTP State Management Mechanism, RFC2169 1997

Marchiori, M. 2002. The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification. Marchiori M., Ed. Available online at http://www.w3.org/TR/P3P/ (2002).

Marx, G. 2003. Technology and Gender: Thomas I. Voire and the Case of the Peeping Tom. The Sociological Quarterly, Volume 43, Number 3, pp. 407-433.

Mayer-Schonberger, V. 1997. The Internet and Privacy Legislation: Cookies for a Treat?, 1 West Virginia Journal of Law & Technology 1,1.

Microsoft, 2001. Internet Explorer 6 Technical Overview. Retrieved from the World Wide Web July, 2003. http://www.microsoft.com/windows/ie/techinfo/overview/default.asp. Posted October 08, 2001.

OED. 2003. Oxford Dictionary. Oxford University Press.

Raiu, C. 2003. Personal Correspondence. Used with permission.

Shipp, A. 2003. Personal Correspondence. Used with permission.

Stefnisson, S. 2003. Personal Correspondence. Used with permission.

Symantec, 2002. Symantec Security Response. Analysis of W32.Bugbear@mm. Available online at http://www.symantec.com/avcenter/venc/data/w32.bugbear@mm.html

Websters, 2003. Websters Unabridged Dictionary.

Whalley, I. 2003. Personal Correspondence. Used with permission.

About the Author

Sarah Gordon is Senior Research Fellow at Symantec Security Response. Her current research areas include testing and standards for antivirus and security software, privacy issues, cyberterrorism and psychological aspects of human/computer interaction.

The has been featured in diverse publications such as IEEE Monitor,The Wall Street Journal, and Time Digital, and profiled by PBS, ITN, and CNN International. Her work has appeared in publications such as Information Security News and Virus Bulletin; she has won several awards for her work in technology. She is a highly sought-after speaker, having presented at conferences ranging from DEFCON to Govsec.

She was recently appointed to the Editorial Board for Elsevier Science Computers and Security Journal. She is on the Advisory Board of Virus Bulletin, and is co-founder and board member of The WildList Organization International. She is Technical Director of The European Institute for Computer Antivirus Research - where she also serves on the Board of Directors and Conference Program Committee. She is a member of SRI's cyberadversary working group.

Sarah was responsible for security testing and recommendation for The United Nations, and participates in various initiatives for Homeland Security and Infrastructure Protection. She was chosen to represent the security industry in "Facts on File: Careers for Kids who Like Adventure", and is a reviewer for various technical security book publishers including Wiley publications. Her work in ethics, technology and profiling computer criminals is required coursework in various academic information security programs. She is committed to excellence in information security education, guest lecturing at Universities world-wide on topics ranging from virus writers and hackers to the truth about cyberterrorism.

Sarah graduated from Indiana University with special projects in both UNIX system security and ethical issues in technology. She is a member of the American Association for the Advancement of Science, The American Counseling Association, and the Association for Family Therapy and Systemic Practice in the UK. Prior to joining Symantec, she worked with the Massively Distributed Systems Group at IBM's Thomas J. Watson Research Laboratory in New York in the AntiVirus Research and Development Team. She may be reached at sgordon@symantec.com.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product information
In the U.S. call toll-free
800.745.6054

Symantec has worldwide operations in 36 countries. For specific country offices and contact numbers please visit our Web site.