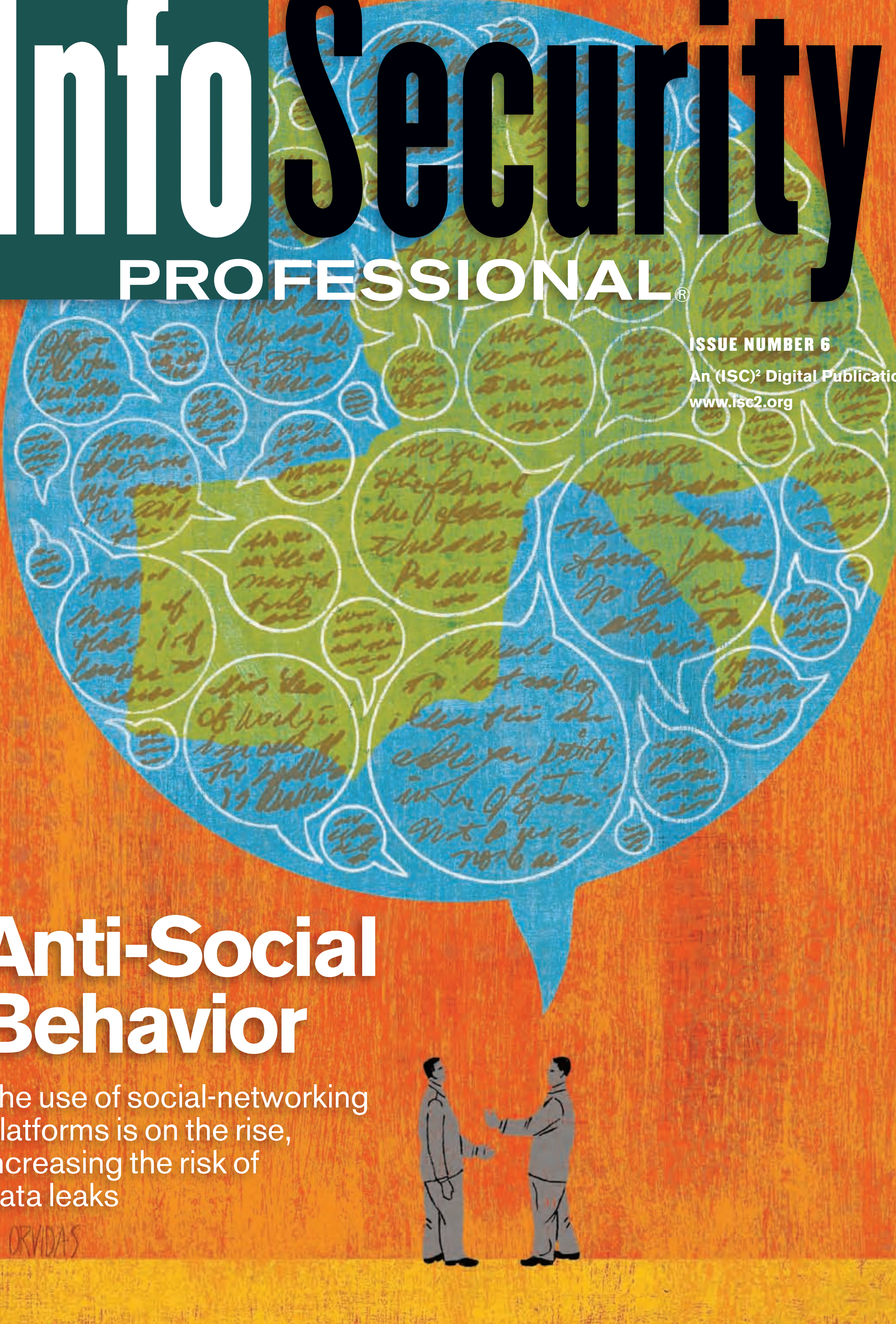
InfoSecurity PROFESSIONAL®

ISSUE NUMBER 6

An (ISC)² Digital Publication

www.isc2.org



Anti-Social Behavior

The use of social-networking platforms is on the rise, increasing the risk of data leaks

Googling Security and Privacy

It's no secret that Google retains search data and metadata regarding searches—in fact, it's quite open about doing so. What's unsure, though, is the long-term threat to information security and privacy.

Let's review Google's elements.

The search giant saves a lot of information. Here's what you should know.

Google Search: This search engine is gathering many types of information about online activities. Its future products will include data gathering and targeting as a primary business goal.

All of Google's properties—including Google Search, Gmail, Orkut and Google Desktop—have deeply linked cookies that will expire in 2038. Each of these cookies has a globally unique identifier (GUID) and can store search queries every time you search the Web. Google does not delete any information from these cookies.

Therefore, if a list of search terms is given, Google can produce a list of people who searched for that term, which is identified either by IP address or Google cookie value. Conversely, if an IP address or Google cookie value is given, Google can also produce a list of the terms searched by the user of that IP address or cookie value.

Orkut: Google's social-networking site contains confidential information such as name, email address, phone number, age, postal address, relationship status, number of children, religion and hobbies. In accordance with its terms of service, submitting, posting or displaying any information on or through the Orkut.com service automatically grants Orkut a worldwide, nonexclusive, sublicensable, transferable, royalty-free, perpetual, irrevocable right to copy, distribute, create derivative works of, and publicly perform and display such data.

Gmail: The primary risk in using Gmail lies in the fact that most users give their consent to make Gmail more than an email-delivery service and enable features such as searching, storage and shopping. This correlation of search and mail can lead to potential privacy risks. For example, email stored on third-party servers for more than 180 days is no longer protected by the Electronic Communications Privacy Act, which declares email a private means of communication.

Gmail Mobile: Mobile phones are increasingly being sold with Gmail built in, and if not, it can be downloaded. The questions to ask: How uniquely does your mobile phone identify you as the user, and when was the last time you changed your phone and your identifiers?

Gmail Patents: Gmail's Patent #20040059712 emphasizes "Serving advertisements using information associated with email." This allows Google to create profiles based on a variety of information derived from emails related to senders, recipients, address books, subject-line texts, path name of attachments and so on.

Google Desktop: Google Desktop allows users to search their desktops using a Google-like interface. All word-based documents, spreadsheets, emails and images on a computer are instantly searchable. Index information is stored on the local computer. Google Desktop 3 allows users to search across multiple computers. GD3 stores index and copies of files on Google's servers for nearly a month.

Chrome: Chrome is Google's browser. It's available for download today and will eventually be installed on new PCs. Some of the risks it poses include:

- Every URL visited gets logged by Google
- Every word, partial word or phrase typed into the location bar, even if you don't click the Enter/Return button, gets logged by Google
- Chrome sends an automatic cookie with every automatic search it performs in the location bar.

Android: Android is Google's operating system for cell phones. It retains information about dialed phone numbers, received phone-call numbers, Web searches, emails and geographic locations at which the phone was used.

Google Health: This product allows consumers—such as employees, coworkers and customers—to store their health records with Google. Recently, CVS Caremark, along with Walgreens and Longs Drugs in the United States, agreed to allow Google Health users to import their pharmacy records.

Organizational Threats

Uninstalling these products or using competitive tools can mitigate many of these threats. But what about the dangers to your organization? One example is Google Search with its Google Flu Trends (www.google.org/flutrends).

Google has correlated flu data from the U.S. Centers for Disease Control (CDC) from 2003 to the present with its own search data. Spikes in users' searches about flu treatments correlated tightly with the CDC data. Flu Trends has demonstrated Google's ability to analyze search data for a specific term or set of terms. And it can retain this data and where it came from because Google in its privacy policies states that it records IP addresses.

So, what's to stop Google from analyzing all search data from your organization's networks? What's the difference between analyzing flu trends and "Top 100 search terms from XYZ Corp."? Or what if a company were to correlate regional threats from swine flu with search data from Google Health/Prescription data and then analyze the health of its employees and detect long-term effects?

Overall, the most critical threat is reliance on Gmail—whether the setting is universities, cities, companies or countries switching to Gmail en masse, or the newest employees in the organization using Gmail as their primary or sole email platform.

Questions to ask your security team: How big is the organization's email archive? How many years of emails are saved? If your organization switches its email hosting service to Google Gmail, what happens to the privacy and confidentiality clauses in your employee and customer contracts?

Another area of concern for hosted email is the potential of having to turn that data over to the government. Google, Yahoo and Microsoft have a history of complying with the United States' and foreign governments' requests for information. If such data is turned over, how much corporate security is being eroded?

Consider the amount of money and manpower dedicated to handling Microsoft Windows patches, viruses, spyware and botnet detection. Imagine the impact that reliance on Google products could have on corporate privacy and security.

Raj Goel, CISSP, is chief technology officer of Brainlink International, an IT services firm. He is located in New York and can be reached at raj@goel.com.