

Why isn't Europe suffering a wave of security breaches?

Jay Cline

June 14, 2006 ([Computerworld](#))

Did you hear the one about the German company that had the big security breach? Probably not, because security breaches don't dominate the headlines in *Die Welt*, *Le Monde* or *El Pais* like they do in *USA Today*. Our national preoccupation with identity theft has no equivalent in the Old World. So what's the rub? Are Europeans that much better at privacy and security than we are?

That wasn't the finding of a survey recently released by Ponemon Institute LLC and the law firm White & Case LLP. They asked 47 U.S. and EU multinational companies about eight aspects of their privacy practices: privacy management, data security methods, communications and training, privacy policy, choice and consent, cross-border data transfer, privacy compliance, and customer-dispute resolution. It was the first survey of its kind that I've seen. What did it discover?

Counterintuitive survey results

Surprisingly, U.S. firms scored higher than their EU counterparts in five of the eight disciplines. In the area of privacy management, 52% of U.S. companies said they had dedicated privacy leaders, compared with 35% for European businesses. U.S. privacy leaders also held more senior positions than their European counterparts.

Why is this important? Because senior, full-time privacy leaders are often necessary to lobby for the resources and organizational change needed to prevent information breaches.

U.S. corporations also scored well in data security methods. Hackers have been the leading cause of publicized security breaches in the U.S. for the past two years, according to Privacyrights.org, which tracks these

incidents. To combat this sophisticated threat, advanced security technologies are a must.

Remarkably, the survey found that U.S. companies were more likely than EU firms to implement encryption, intrusion detection and Web site monitoring and to require vendors to comply with data security obligations.

Employee training is another key component in preventing information breaches. Employee error -- such as e-mailing sensitive information to the wrong people or discarding computers without erasing the personal information stored on them -- has been the second leading cause of publicized breaches in the U.S.

Yet U.S. companies are doing relatively better in this area too, with 54% of U.S. firms offering privacy awareness and training programs for their employees, compared with 32% for those based in the EU.

So if U.S. companies are better than the Europeans at key privacy and security practices, why are there so many more publicized breaches in America?

The dearth of EU breaches

That's the question I posed to 50 privacy experts in North America and Europe. Their answers fell into three camps, with most citing more than one factor:

1. **U.S. under the microscope.** The overwhelming majority --- 85% -- attributed the discrepancy to higher reporting standards, litigiousness and media focus in the U.S. Nearly 40 U.S. states now require public notification of security breaches, while EU member states have only started to consider this requirement.

This means that Europe could be experiencing just as many breaches as the U.S., but several factors make it more likely that U.S. breaches will be publicized. Indeed, 94% of the EU companies surveyed by Ponemon/White & Case reported that they had

experienced a breach in the past three years, compared with 86% for the U.S. sample.

"Recently, I spoke at a conference where the head of an EU data protection authority chided the U.S., stating that in his country, far fewer breaches occurred," said David Bender, head of White & Case's global privacy practice. "But he had no way of knowing that, because there they don't have requirements to disclose breaches publicly."

2. **EU less exposed.** A third of the experts said that the EU is strong at other privacy methods and that EU companies' data practices are more limited and not as exposed to breaches. The survey did find several data practices that EU firms do well:
 - Providing employees with choice or consent on how information is used or shared (54% for the EU versus 32% for the U.S.).
 - Imposing a strict "no-share policy" for consumer data (50% for the EU, 10% for the U.S.) and employee data (89% for the EU, 28% for the U.S.).
 - Maintaining rigorous controls on cross-border data transfer (54% for the EU, 36% for the U.S.).
 - Monitoring compliance with privacy policies (61% for the EU, 59% for the U.S.).

"Most companies in Europe use much more robust methods of identification," said Intel Corp.'s Munich-based director of privacy and security policy, David Hoffman, "and they discourage the use of a national ID number as an identifier, taking away much of its potential to cause harm if stolen."

Our experts not only see the EU excelling at several use restrictions on personal data; they also see less data collection in Europe. "Our benchmarks show that European companies collect less personal information about customers," Larry Ponemon, founder of the Ponemon Institute, told me, "and [they] are less likely to use this information for unrelated, secondary purposes."

3. **U.S. more targeted.** A third of this expert group saw the flip side of the coin of limited data collection. With more expansive data profiling and sharing in the U.S., criminals find the U.S. a more lucrative target. It's also home to many dot-coms that are most efficient at processing credit card payments to deliver products and services to U.S. addresses, an attractive conduit for using stolen information.

Peggy Eisenhauer, founder of Privacy and Information Management Services, echoed a theme several experts raised. "In the U.S., we have a very developed consumer-credit market, with instant credit and remote purchasing on credit being a norm," she said. "This means that ID theft is an easy and profitable crime."

Outlook

If there's merit to all three of these arguments, what will the future hold? I think the most important variable is whether European companies increasingly adopt the high-risk, high-return business model of data aggregation and Internet commerce. If they do so without adding more of the U.S.-style controls, they'll suffer an even worse outbreak of ID theft, and the public there will certainly clamor for more public notice of breaches. Multiply the U.S. experience by two.

On the other hand, U.S. firms are also at a crossroads. Their current level of publicized breaches can't sustain consumer confidence in e-commerce. Unless they adopt more of the EU-style controls, consumers will start switching to cash-only transactions, and the Internet will become simply a big search engine.

Which will happen first? I think the latter, because of the "Pain Principle." The Pain Principle says that organizations change only when something is causing them pain, and U.S. businesses are certainly feeling more privacy pain right now. Coming through this rough spot, with more information controls in place and restored customer trust, may give U.S. companies a needed competitive edge to succeed in the next round of the Information Age.

Jay Cline manages data privacy at Carlson Companies Inc., a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. These are his views and not necessarily those of Carlson, and should not be taken as legal advice. Contact him at cwprivacy@computerworld.com.