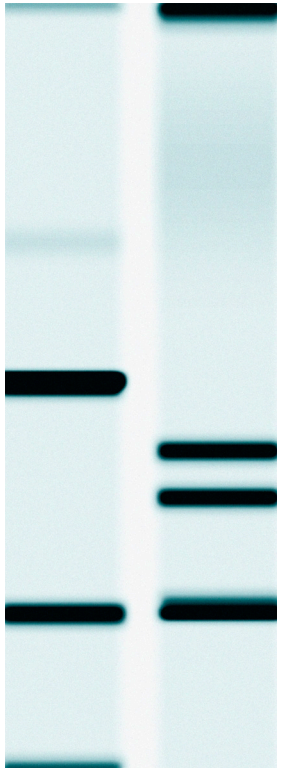
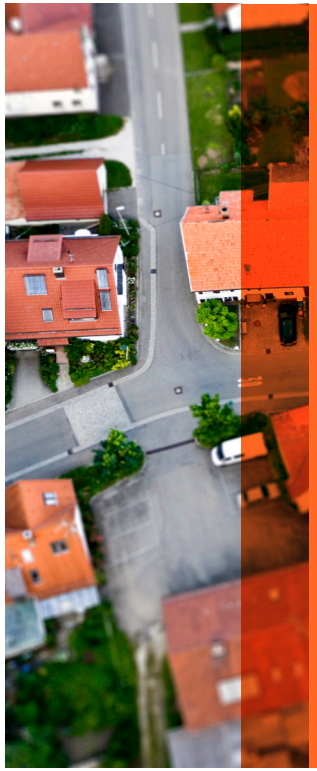
Security, Privacy, and Web 2.0





A GLOBAL
INNOVATION
OUTLOOK
REPORT

Security, Privacy, and Web 2.0

Balancing the security risks and business rewards of the interactive Web

About 20 years ago, the world was introduced to an extraordinary new medium of communication called the World Wide Web. Over the ensuing years, as adoption spread, the Web quickly and radically revolutionized the way we live and work. It introduced a new and powerful medium of social, political, and economic transaction.

Before the world could catch its collective breath from this change, Web 2.0 added a new level of interactivity to the medium. This ability to openly exchange information—to buy and sell, to consume and create—gave rise to an explosion of social and economic creativity: Web-based communities; blogs; wikis; online auctions; social-networking sites; and video-sharing sites.

Web 2.0 exponentially increased the transactional nature of the Web, and forever changed the way people express themselves, conduct business, learn about different subjects, shop, form communities, collaborate, and share their personal information.

But the embrace of Web 2.0 has also introduced serious questions about the inherent risks associated with the use of these tools. For example, what are the expectations of privacy on Web 2.0 sites? Which types of personal and work information are safe to disclose? How can consumers protect themselves against identity theft, cybercrime, and abusive marketing? When is online surveillance appropriate? What role should traditional regulatory and law enforcement organizations play? And what are the guidelines for use of Web 2.0 in the workplace?

This report is based on a survey developed and conducted by the Ponemon Institute and IBM's Global Innovation Outlook. The survey was given to more than 3,000 consumers around the world in an effort to discern the awareness of these issues among users of Web 2.0 applications and to identify the steps that businesses can take to protect themselves and their employees from the associated risks. In learning more about what security and privacy factors increase or decrease use of Web 2.0, both at home and in the workplace, developers of Web 2.0 applications can more proactively address security concerns, increasing the usage and usefulness of their sites. And employers can craft policies on Web 2.0 use that both increase the value to the company and limit risk.

Among the conclusions drawn from this report:

> Geography and culture play important roles in determining risk tolerance for Web 2.0 applications, and must be taken into account when crafting usage guidelines. This is especially true for global employers.

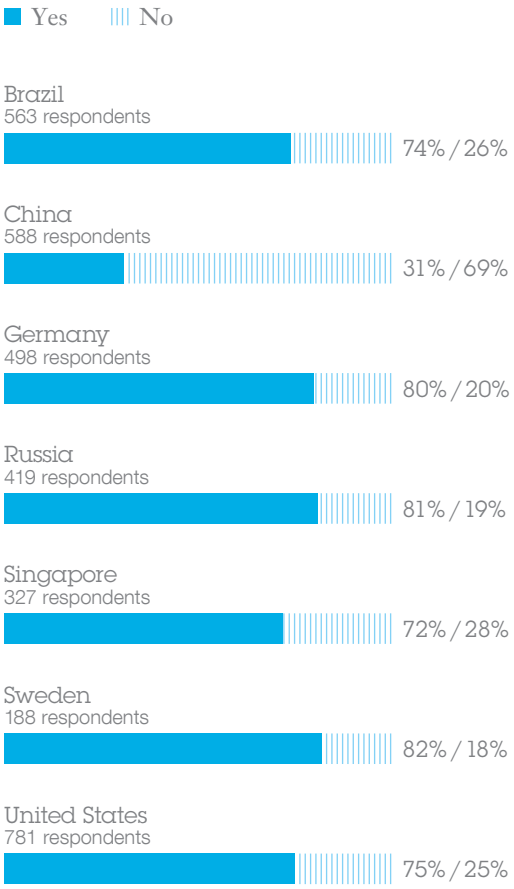
> The nature of Web 2.0 content, and its perceived benefit to the end user, greatly affects a user's willingness to assume security risks.

> There is an inherent distrust of traditional forms of regulation or law enforcement among Web 2.0 users, making attempts to artificially control or restrict use among employees likely to backfire.

> Transparent privacy policies and the ability to control one's own privacy and security settings greatly increase use of Web 2.0.

> Employers can leverage the naturally cautious instincts of Web 2.0 users and allow employees to develop their own usage policies and guidelines.

Do you use social networks, social messaging, blogs, wikis or other Web 2.0 tools on the Internet?

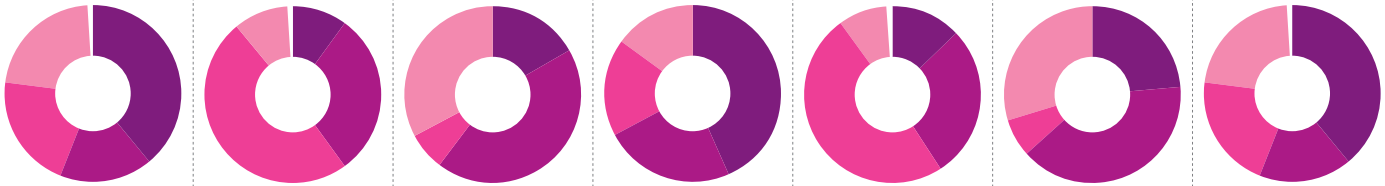


About the Survey

The survey was conceived and conducted through a collaborative effort between IBM's Global Innovation Outlook and the Ponemon Institute. It was taken by 3,364 consumers in seven different countries around the world, including the United States, Brazil, Russia, China, Singapore, Sweden, and Germany.

Respondents were asked a series of questions about their use of social networks, social messaging, blogs, wikis, and other Web 2.0 tools. The purpose was to gain an understanding of what security and privacy factors increase and decrease use of Web 2.0 applications; what users value the most about the applications; and what users are most willing to share online.

Why would you participate in Web 2.0 applications?



	Brazil	China	Germany	Russia	Singapore	Sweden	United States
The benefits from participating outweighs any privacy or security risk	39%	10%	17%	44%	13%	24%	34%
I benefit from exchanging information about myself with other like-minded community members	17%	30%	44%	24%	28%	40%	48%
I believe the security of the Web 2.0 application is adequate in protecting my personal information	21%	49%	7%	18%	49%	7%	11%
I am aware of potential dangers and willing to take steps to protect myself	22%	10%	33%	15%	9%	30%	8%

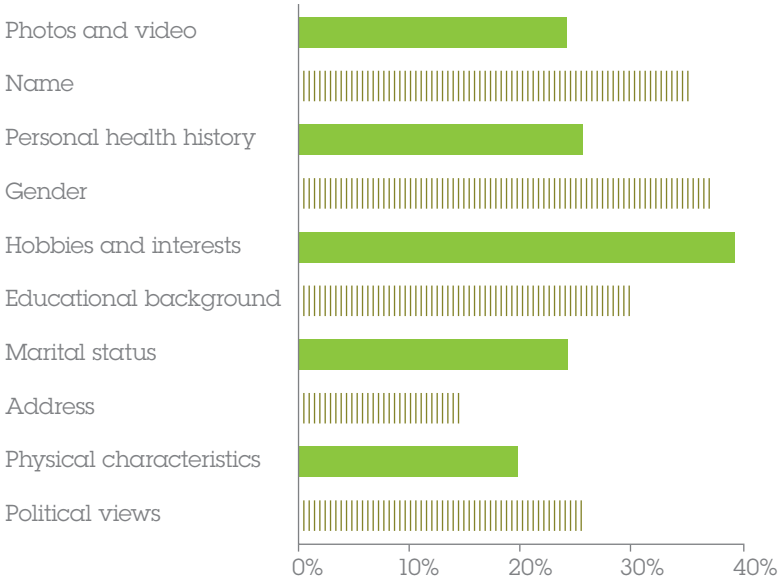
Note: Totals here and throughout document do not equal 100% due to rounding.

The survey reveals that, in general, positive reasons for using Web 2.0 applications include: responsibility for protecting members comes from the online communities themselves and the individuals that belong to them; the amount of personal information required to belong is limited and at the discretion of users; the anonymity of users is optional; and the site provides access to quality and important information.

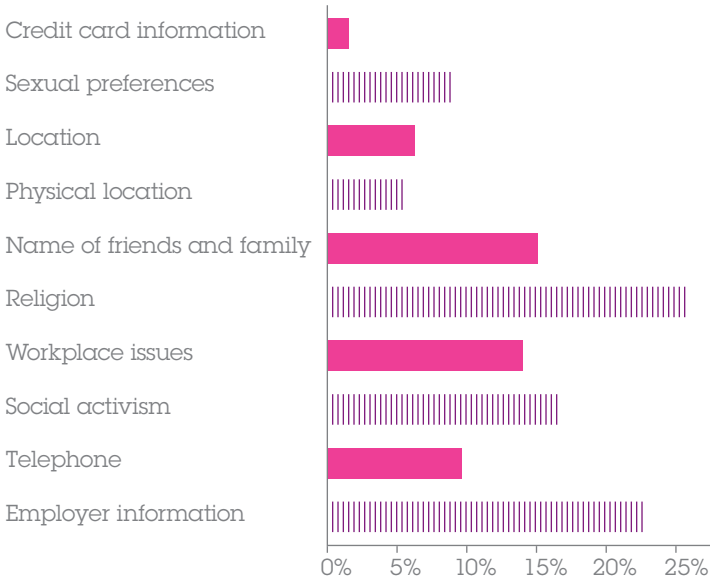
In contrast, reasons for not using Web 2.0 are: regulations and protection of members is the responsibility of the government; behavior can be monitored by law enforcement; users are asked to provide information about their credit card, location, sensitive health issues (i.e. addictions), names, and sexual preferences.

Taken together, the responses to the survey tell the story of the compromises Web 2.0 users are willing to accept in order to reap the benefits of these applications. These trade-offs, and the point at which users are no longer willing to accept the inherent risks of Web 2.0 services, are a moving target, shifting over time as new services are introduced and social norms evolve. But at any point in time, that breaking point can be measured.

Data types users are **most** willing to share in Web 2.0 environment.



Data types users are **least** willing to share in Web 2.0 environment.



The Tipping Point Resiliency Index (TPRI)

To measure overall resiliency to security concerns, respondents were given four different scenarios in which the benefits of a popular Web 2.0 service are weighed against the potential risks.

The scenarios included:

> A social network on health and wellness where users share information about their medical conditions and treatments. This network is potentially subject to unauthorized use by employers, insurance companies, and government agencies.

> A free social messaging utility that allows users to communicate and share information, photos and news about themselves or others. This utility is subject to potential marketing or advertising abuse.

> An online community for business professionals interested in volunteering their time for good causes. The community has had problems with members sharing confidential information about their employers, including financial statistics and product research.

> A corporate wiki designed to create a sense of community between employees, especially those in remote locations. The wiki has seen some employees post uncensored content, including unflattering photos and criticism of colleagues and confidential company information.

Tipping Point Resiliency Index

	Brazil	China	Germany	Russia	Singapore	Sweden	United States	Average
Social network for health and wellness								
Before incident: Will you use this?	73	31	46	41	32	46	54	46
After incident: Will you use this?	78	73	36	51	72	38	61	58
Net	5	42	-10	10	40	-8	-7	12
Free social messaging								
Before incident: Will you use this?	72	57	54	52	59	48	54	57
After incident: Will you use this?	52	34	27	56	26	30	41	38
Net	-20	-23	-27	4	-33	-18	-13	-19
Online community for social and business activities								
Before incident: Will you use this?	58	20	59	47	31	57	54	47
After incident: Will you use this?	50	13	27	50	16	32	31	31
Net	-8	-7	-32	3	-15	-25	-23	-15
Wiki in the workplace								
Before incident: Will you use this?	56	20	54	31	26	53	47	41
After incident: Will you use this?	33	31	25	37	38	20	40	32
Net	-23	11	-29	6	12	-33	-7	-9
Overall								
Before incident: Will you use this?	65	32	53	43	37	51	52	48
After incident: Will you use this?	53	38	29	49	38	30	43	40
Net	-12	6	-25	6	1	-21	-9	-8
Rank order on resilience measures	4	1	6	1	2	5	3	

*Rates = expressed as percentage × 100; Participation rate in scenario before data security incident = X; Participation rate in scenario after data security incident = Y (for those that answered affirmatively above)
Resiliency score is established as the difference termed R = {Y - X}; For R > 0; resiliency is high and for R ≤ 0 resiliency is low.

TPRI Conclusions

From the TPRI results, we can make a few assumptions as they relate to how private enterprises should approach Web 2.0 matters.

> Different geographies have vastly different tolerance levels for security and privacy risk with Web 2.0. This implies that a single, worldwide policy on Web 2.0 usage may not be advisable for global firms looking to encourage use. Policies must be locally tailored to suit the cultural norms of a region.

> The value and personal relevance of content is critical to adoption of Web 2.0 technologies. Even in the least resilient locations (Germany and Sweden), health and wellness content greatly increased the willingness of users to accept vulnerability. But even this is subject to geographical variance.

> Resiliency is lower than average among those that use Web 2.0 at work. This indicates that users understand the risks associated with revealing both personal and business information in a work environment. They show a natural inclination to exercise caution, especially when working with uncensored content or confidential company information.

Who, What, and Where

The three factors of resiliency

Based on the results of the Tipping Point Resiliency Index, and supported by various other questions from the survey, there are at least three major factors that shape an individual's resiliency to security and privacy risk when using Web 2.0 applications. These are the "Who, What, and Where" factors of community, content, and culture.

Who

A sense of **familiarity and common interests** is critical in bolstering resiliency. Respondents were more likely to increase their use of a Web 2.0 application, despite perceived security and privacy risks, if they shared thematic interests with others in the community.

64%

of respondents say they would increase their use of a free social messaging utility if it connected them with members who share common likes, tastes, and preferences.

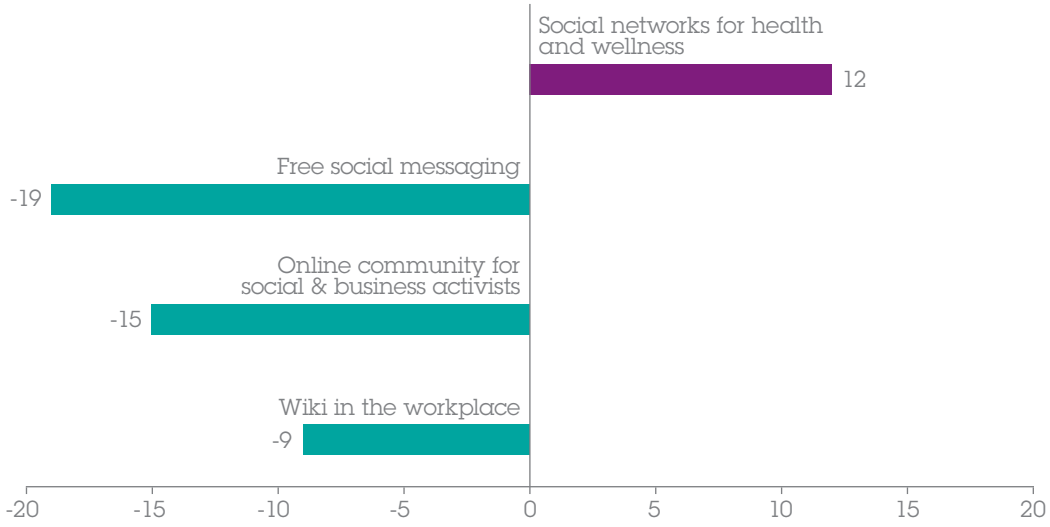
44%

of respondents say they would increase their use of a workplace wiki if it provided an opportunity for employees to maintain contact with others who share a common set of values, interests, and preferences.

What

The **type of content** a Web 2.0 application offers makes a significant difference in how committed users stay to the service, and what kind of information they are willing to divulge. Resiliency is increased by the **perceived value of the site,** and the type of information divulged is affected by the nature of the content.

Average resiliency scores



49%

of Chinese and Singaporean respondents said they use Web 2.0 applications because they believe the security of the application is adequate in protecting their personal information.

Only 7%

of Swedish and German respondents said the same.

Where

Geographical and cultural differences have a major impact on resiliency scores. In general, European Union countries have the lowest tolerance for security and privacy risk, while Asia and Russia have the highest.

Country	Resiliency Rank	Score
Brazil	4	-12
China	1	6
Germany	6	-25
Russia	1	6
Singapore	2	1
Sweden	5	-21
United States	3	-9

Responsibility and Risk

Web 2.0 communities favor self-policing, transparency and control

True to the progressive, empowering nature of Web 2.0 applications themselves, users of these services have progressive, and still evolving, views on who should be responsible for ensuring their security. In many cases, respondents believe that individuals or the communities themselves should bear the responsibility for security.

In some of the more community-oriented sites on the Web, this is already happening. “In World of Warcraft, for example, players assign each other rankings based on reputation and contribution,” says Gunter Ollman, chief security strategist at IBM Internet Security Systems. “If someone insists on being disruptive and not playing by the rules, they will find themselves quickly ostracized by the group. There are even organized ‘vigilante’ groups that will track down chronic abusers of the rules, regardless of changes in their in-game identities, and publicly post records of their behavior as a warning to others. Once you build up a bad reputation, it becomes very hard to escape it.”

But here especially, there are significant regional differences.

Who do you believe is most responsible for ensuring a safe Internet? Please rank the following list from 1 = most responsible to 5 = least responsible.

	Brazil	China	Germany	Russia	Singapore	Sweden	United States	Average
Individual users	2.10	3.71	3.90	2.08	3.34	3.82	2.03	3.16
The online community as a whole	3.50	3.13	2.76	3.15	3.43	2.78	2.99	3.12
Internet service provider	4.32	3.96	4.04	4.25	3.95	4.42	4.21	4.16
Law enforcement	4.10	3.55	3.16	4.25	3.39	3.33	4.56	3.63
Government	3.71	2.22	2.55	3.44	3.18	2.79	3.42	2.98

One thing that all regions agree on is that the online communities themselves should take significant steps to **protect their members**. Setting standards for acceptable behavior, enforcing compliance with those standards, and implementing security tools to detect and prevent noncompliance are among the basic services users expect. And by allowing for anonymity among users, limiting the amount of personal information required to join, and developing clear and transparent policies on security and privacy, user concerns can be further assuaged.

"I think that privacy is too often juxtaposed with security, and it's assumed that security means that you're giving up privacy," says Chris Kelly, chief privacy officer at Facebook. "But I think you can have a great deal of control over your personal information and still maintain a secure environment. In fact, having that control can result in a more secure environment."

For its part, Facebook recently overhauled its security and privacy controls. In an open letter from founder Mark Zuckerberg to all 350 million users of the service, the popular social networking site added the ability to control who sees each individual piece of information on a person's profile. The open letter speaks to the kind of transparency Web 2.0 users are looking for, and the changes to the privacy settings are exemplary of the level of control users demand.

Do you believe the online community should take steps to protect its members?

Yes | No

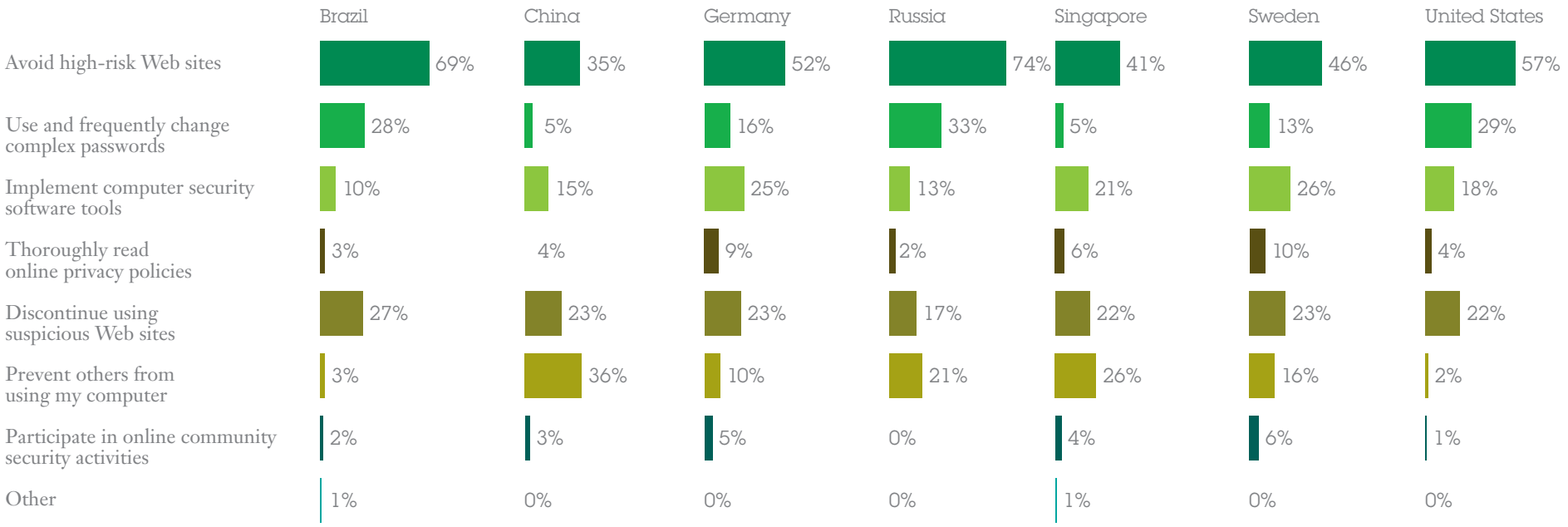
Brazil 563 respondents	China 588 respondents	Germany 498 respondents	Russia 419 respondents	Singapore 327 respondents	Sweden 188 respondents	United States 781 respondents
74% / 26%	73% / 27%	81% / 19%	57% / 43%	74% / 26%	76% / 24%	80% / 20%

If yes, how would this work? *(Top two choices).*

	Brazil	China	Germany	Russia	Singapore	Sweden	United States
Set a code or standards that specify(ies) acceptable behaviors	34%	12%	37%	23%	19%	57%	23%
Educate members about how to avoid potential harms	19%	24%	34%	26%	31%	37%	18%
Enforce compliance with acceptable standards of behavior	50%	34%	30%	53%	26%	23%	37%
Implement security tools to detect and prevent undesirable behavior	46%	35%	54%	20%	40%	19%	44%
Demand social network provider to have better safeguards in place	15%	16%	11%	13%	10%	26%	23%
Monitor online activities to detect threats	21%	26%	23%	45%	25%	16%	20%
Work with law enforcement to police Web site for suspicious activity	15%	49%	10%	18%	46%	16%	33%

While it's true that Web 2.0 users are demanding control, it's not always clear that delivering that control will result in more secure online behavior. For example, there is a definite limit to what individual users are willing to do to ensure their safety and security. Users are most willing to avoid high-risk or suspicious Web sites; less willing to familiarize themselves with online privacy policies or participate in community security activities.

What are you willing to do in order to ensure online safety and security?



Still, experts believe that over the long run offering users control and transparency, regardless of whether they take advantage of it, will create a more trusting and secure user base.

"We know that empowering people to take responsibility for their own assets is an important part of delivering security; users are part of the system and so will inevitably have a positive or negative effect on vulnerability and exposure to threats," says Sadie Creese, director of e-Security at the University of Warwick Digital Library.

"By enabling people to take effective control over their personal information we can begin to limit the level of vulnerability they have to identity theft and associated crime. This in turn has benefits for wider society as it will help to prevent fraudulent access to corporate assets and citizen services, and play a part in fighting organized crime and terrorism."

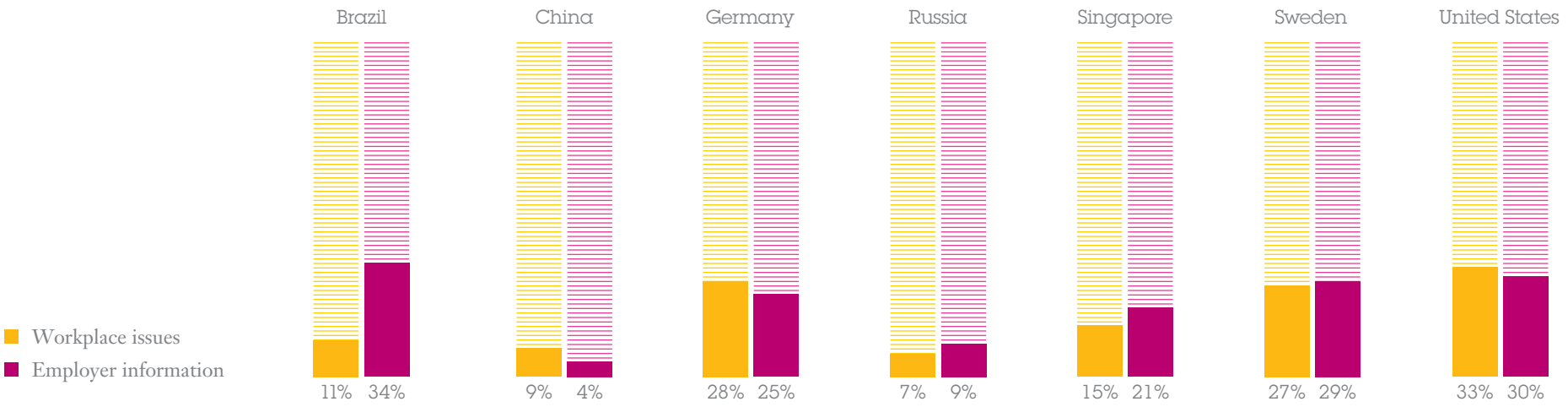
Web 2.0 and the Workplace

Sharing information, inside and outside of the office

Early on, many corporations tried to limit the use of Web 2.0 applications from within the company firewall. They feared the applications would weaken security, provide an outlet for confidential information, and drain endless hours of productive time from employees. Though those fears were not totally unfounded, most companies found that restricting Web 2.0 use among employees was neither practical nor reasonable. And since then, a combination of external and internal Web 2.0 usage has sprouted throughout corporate networks all over the world.

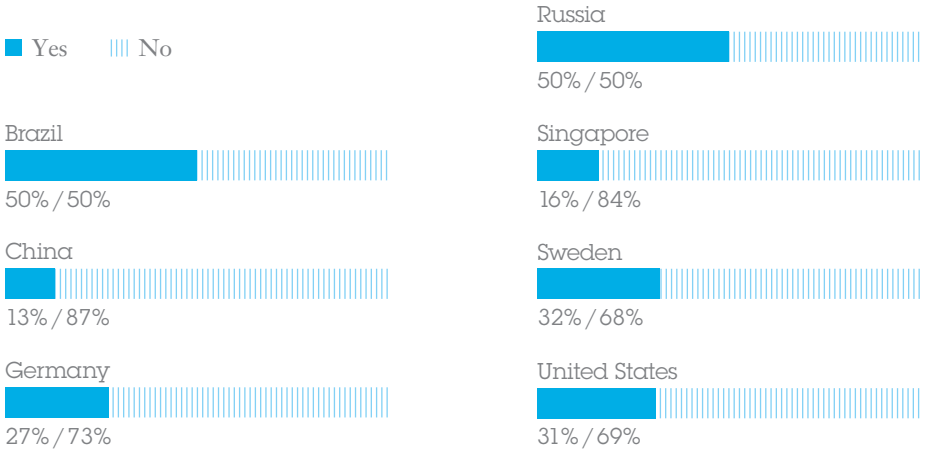
Guidelines for appropriate behavior and use of these applications within a corporate setting are still evolving. Sometimes these guidelines are set by a company; sometimes by a department manager; and sometimes they are not set at all. Some companies are embracing the spirit of Web 2.0 and allowing their employees to work collaboratively to set their own guidelines and behavioral expectations. Several years ago, IBM used a wiki to develop its corporate blogging policy, soliciting input from all of its 400,000 employees. The company has since extended the same approach to other Web 2.0 technologies.

Global respondents that are willing to share workplace issues or employer information on a social network community



Many employers have come to see the value of Web 2.0 applications in the workplace, both for the purposes of working and communicating with the outside world. And common sense has led most Web 2.0 users to observe the same rules of the road they would in any other circumstance. In general, that means a healthy dose of caution, especially when posting information on an external site.

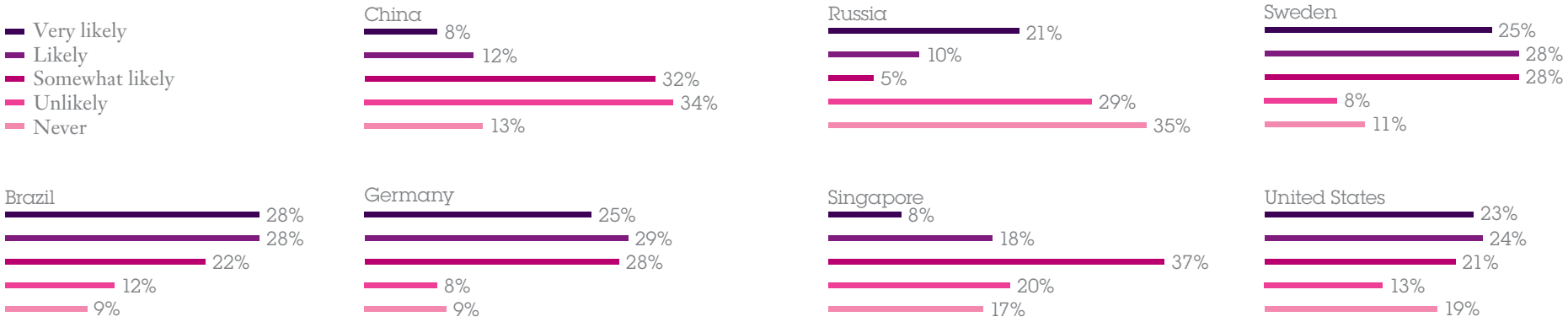
Would you still consider using a social network knowing that it creates a risk to the security of confidential data about your company?



When it comes to using Web 2.0 applications that are specifically designed for the corporate setting, respondents are circumspect. In general, employees are willing to use a wiki that enables them to share information about themselves and their work.

The list of reasons why an employee would use a workplace wiki is long and varied. But across the board, respondents agreed that relevant and timely information about the company in which they work was a strong incentive for using the application. Other factors that increased use were the development of a sense of community and the ability to control the content that identifies them.

How likely would you be to use a wiki that enables you to share information about yourself and your work?



Interestingly, the ability to post content anonymously ranked high among these responses. But in other survey questions, respondents indicated they are likely to willingly share personal information about themselves. This demonstrates that users of Web 2.0 applications appreciate and value the option to remain anonymous, even if they choose not to exercise it. It increases their trust in the provider of the service.

The following is a list of possible factors that may affect your use of this wiki.
Adjacent response = increase use

	Brazil	China	Germany	Russia	Singapore	Sweden	United States
The wiki provides relevant and timely information about the organization.	66%	43%	63%	59%	46%	69%	51%
The wiki provides opportunities for employees to organize and unite on critical issues.	48%	4%	56%	49%	18%	57%	40%
The wiki provides an opportunity for employees to maintain contact with others who share a common set of values, interests and preferences.	59%	21%	51%	41%	26%	68%	62%
The wiki provides opportunities to freely communicate issues and concerns with the organization's management.	53%	5%	58%	17%	25%	59%	40%
The company provides clear disclosure about posting content that may make others feel uncomfortable.	22%	14%	44%	20%	18%	40%	43%

(continued)

	Brazil	China	Germany	Russia	Singapore	Sweden	United States
The company ensures anonymity wherein the employee's identity cannot be determined when he or she posts content to the wiki.	49%	50%	59%	50%	54%	62%	59%
The company implements strict authentication over who is able to post content to the wiki.	60%	71%	50%	63%	57%	43%	52%
The company sets standards about the posting of business information.	24%	33%	50%	20%	37%	57%	39%
The company censors all content before posting to the wiki.	10%	47%	40%	14%	40%	38%	25%
Employees have the ability to control, modify or delete any content that identifies them.	77%	20%	65%	50%	36%	55%	69%
The community of wiki users set standards of acceptable behavior.	25%	30%	53%	20%	35%	52%	36%
The community of wiki users establishes a governance body to hear complaints and enforce standards.	19%	48%	43%	15%	33%	38%	38%
The community of wiki users establishes an employee group to censor content before posting.	16%	55%	39%	22%	49%	39%	38%
Goverment sets regulations that restrict companies from using wikis that may reveal an employee's personal information.	16%	39%	31%	10%	45%	39%	40%

The role an employer plays in engendering trust and respect among participants in these applications is critical if they are to be of value to the overall operation. The example of IBM using a wiki to develop company blogging policy is again relevant here. In this case, the company did not presume to know the best way to manage these still-developing tools. Yet the guidelines that result invariably follow well understood, long-standing corporate policies and common sense.

"These are rapidly evolving areas of communication and interaction. Our employees understand many of the associated security and privacy risks," says Harriet Pearson, vice president security counsel and chief privacy officer at IBM. "Empowering employees to help develop guidelines engenders trust, fosters the enterprise-wide learning process, and improves compliance."

Conclusion

The success and longevity of Web 2.0 is no longer in question; it is a model that will be with us for a long time to come. But the extent to which a Web 2.0 application can foster collaboration and innovation within and between companies depends on the security comfort-level of its user base.

To address this effectively, organizations should consider the cultural and regional expectations of privacy and craft policies that reflect them. They should employ Web 2.0 services only where they will deliver tangible value to end users. And they should give employees an active role in both creating usage guidelines and enforcing them.

Using the insights generated from this study, developers and employers can build sensible security provisions and maximize the value of their Web 2.0 applications. And maybe even pave the way for the next evolutionary step of the World Wide Web.

About the Ponemon Institute

Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

About the GIO

Over five years ago, IBM launched a unique experiment in exploration, collaboration and innovation: the Global Innovation Outlook (GIO). During its evolution, we've convened hundreds of thought leaders, policy makers, business executives, university researchers and representatives from nonprofit organizations. We've explored topics as varied and important as healthcare, energy and the environment, economic development in Africa, and the future of the world's water resources. We've shared the results of our exploration and analysis through reports and studies, brokered new relationships, and launched dozens of collaborative initiatives among GIO participants.

The idea of the GIO emerged from a central insight and belief about 21st century innovation, one that was enthusiastically validated across every session we held in its inaugural year: innovation is no longer a solitary exercise. Instead innovation will increasingly need to be open, intensely collaborative, multidisciplinary and global in its reach and impact. Today this belief pervades just about

all IBM interactions. It is clearly visible in our thinking about building a Smarter Planet, and our implicit invitation for like-minded people around the world to join us in this endeavor.

Engage with IBM at any level today, and you will witness this belief in action, as well as the culture it engenders. It's how we do business, how we get things done—how we help make the world work better. So in a sense, the GIO itself is no longer necessary as a stand-alone program, and so we will no longer be conducting separate GIO deep dives, round tables or forums as such. We will, however, continue to support and cultivate the communities essential to the spirit of the GIO, including the GIO Facebook and LinkedIn communities, so that GIO alumni can contact each other and IBM as often as they wish. GIO reports and other collateral material will also remain available. And the GIO blog archives will continue to be hosted at http://www.gio.typepad.com/.

If we've been fortunate enough to have you participate in one of our GIO sessions, we trust that the people you've met and the topics you've discussed have been extremely valuable to you and your organization. And we encourage you to continue to engage with us at IBM, as well as with your fellow GIO Alumni.

International Business Machines Corporation
New Orchard Road, Armonk, NY 10504

Appendix: Audited Findings

Countries	Brazil	People's Republic of China	Germany	Russian Federation	Singapore	Sweden	United States
Abbreviated Country	BZ	CH	DE	RF	SG	SW	US
Panel	14,083	19,001	8,049	11,620	6,780	3,512	15,998
Sample	563	588	498	419	327	188	781
Response	4.0%	3.1%	6.2%	3.6%	4.8%	5.4%	4.9%

Do you use social networks, social messaging, blogs, wikis, or other Web 2.0 tools on the Internet?

	BZ	CH	DE	RF	SG	SW	US
Yes	418	183	400	339	235	155	586
No (Stop)	145	405	98	80	92	33	195
Total	563	588	498	419	327	188	781

If yes, how are you using these Web 2.0 applications? Please select all that apply.

	BZ	CH	DE	RF	SG	SW	US
Performing search	356	85	356	250	185	119	418
Obtaining news and information	391	53	367	227	160	135	509
Participating in a social network	187	52	239	187	111	80	290
Using social messaging tools	150	31	201	146	105	75	248
Blogging or contributing to wikis	98	32	95	55	19	49	126
Browsing or shopping	382	89	353	244	201	133	552
Banking or paying bills	56	0	50	23	5	17	398
None of the above (Stop)	18	40	44	24	29	15	24
Total	1,638	382	1,705	1,156	815	623	2,565
Adjusted sample size after screening	400	143	356	315	206	140	562

Responses = strongly agree and agree combined responses on a five-point scale.

	BZ	CH	DE	RF	SG	SW	US
Online communities are responsible for protecting their members.	69%	22%	56%	35%	29%	85%	60%
Social network providers are responsible for protecting their members.	72%	38%	51%	52%	35%	60%	64%
Internet service providers are responsible for protecting their users.	39%	43%	47%	15%	26%	51%	27%
People who don't live up to acceptable standards of behavior should be denied access to online communities.	39%	85%	61%	14%	83%	55%	50%
Individual members and not the community as a whole should take responsibility for ensuring their own safety and security online.	26%	14%	88%	66%	15%	28%	78%
Online community surveillance and monitoring will lead to vigilantism.	23%	19%	49%	57%	37%	41%	43%
Average	45%	37%	59%	40%	38%	54%	54%

Social network on health & wellness

Would you consider using a social network that contributed to your health and wellness? Please use the following scale to indicate how likely you would be to use this Web 2.0 Internet application.

	BZ	CH	DE	RF	SG	SW	US
Very likely	39%	10%	19%	26%	11%	17%	27%
Likely	34%	21%	27%	15%	21%	29%	27%
Somewhat likely	11%	28%	28%	5%	26%	29%	22%
Unlikely	9%	24%	20%	28%	25%	20%	17%
Never	7%	17%	6%	26%	16%	4%	7%

Social network on health & wellness

Please check the information you are willing to share in a social network on health & wellness (for those who said very likely or likely only).

	BZ	CH	DE	RF	SG	SW	US
Name	52%	13%	22%	34%	38%	24%	50%
Address	27%	7%	1%	10%	10%	4%	34%
Telephone	17%	0%	7%	7%	11%	0%	27%
Age	46%	33%	31%	35%	32%	30%	53%
Gender	36%	47%	32%	31%	45%	32%	42%
Race	21%	31%	34%	49%	24%	43%	28%
Religion	18%	30%	36%	53%	24%	41%	34%
Ethnicity	25%	36%	36%	50%	25%	42%	28%
Sexual preference	0%	3%	15%	7%	0%	16%	3%
Physical characteristics such as weight, height	17%	17%	9%	23%	22%	6%	34%
Family health history	49%	36%	20%	23%	40%	19%	44%
Personal health history	42%	36%	12%	10%	10%	5%	47%
Photo & video	12%	13%	18%	31%	19%	8%	54%
Prescription drugs	34%	33%	16%	10%	32%	17%	43%

Social network on health & wellness

(continued)

	BZ	CH	DE	RF	SG	SW	US
Diet	51%	44%	43%	52%	46%	45%	41%
Addictions	6%	0%	0%	4%	2%	3%	3%
Employer information	38%	5%	31%	12%	15%	24%	26%
Interest in clinical trial research	12%	9%	17%	20%	10%	14%	19%
Name of primary health care provider	43%	15%	39%	38%	19%	40%	48%
Health insurance information	3%	0%	0%	0%	0%	0%	37%
Educational background	44%	16%	24%	39%	17%	31%	43%
Credit card or bank payment information	0%	0%	0%	3%	5%	3%	4%
Average	27%	19%	20%	25%	20%	20%	34%

Would you still consider using a social network that contributed to your health and wellness knowing that others may have access to your sensitive health information?

	BZ	CH	DE	RF	SG	SW	US
Yes	78%	73%	36%	51%	72%	38%	61%
No	22%	27%	64%	49%	28%	62%	39%
Total	100%	100%	100%	100%	100%	100%	100%

Social network on health & wellness

The following is a list of possible factors that may affect your use of this social network. *Adjacent response = increase use*

	BZ	CH	DE	RF	SG	SW	US
The social network helps members to find high-quality physicians and other medical specialists.	87%	64%	59%	91%	64%	52%	85%
The social network provides opportunities to obtain free medical services.	82%	42%	31%	83%	40%	22%	64%
The social network provides opportunities to earn income through participation in clinical trial research.	44%	21%	19%	45%	19%	18%	22%
The social network provides substantial discounts on major health products and insurance.	87%	56%	55%	85%	57%	46%	85%
The social network provides clear disclosure about the possible risks of sharing personal health information.	22%	34%	45%	13%	34%	46%	39%
The social network ensures anonymity wherein the user's personal identity cannot be determined.	48%	51%	55%	50%	52%	61%	60%

Social network on health & wellness

(continued)

	BZ	CH	DE	RF	SG	SW	US
The user has control over who sees or has access to personal information.	57%	43%	53%	46%	42%	61%	55%
The social network imposes strict authentication over who is able to join the online community.	63%	61%	48%	62%	59%	42%	55%
Members of the online community set standards of acceptable behavior.	30%	28%	48%	16%	32%	49%	41%
Members of the online community establish a governance body to hear complaints and enforce standards.	17%	47%	39%	17%	37%	43%	36%
Members of the online community establish a group to monitor for suspicious activities.	37%	39%	22%	48%	39%	19%	39%
Law enforcement (police) monitors online community for suspicious activities.	15%	46%	44%	17%	44%	40%	30%
Government sets regulations that require the social network to implement security measures.	24%	37%	38%	17%	39%	40%	28%

Free social messaging

Would you consider using a social messaging utility that enables you to communicate with your colleagues, friends and family? Please use the following scale to indicate how likely you would be to use this Web 2.0 Internet application.

	BZ	CH	DE	RF	SG	SW	US
Very likely	38%	29%	29%	27%	31%	18%	28%
Likely	34%	28%	25%	25%	28%	30%	26%
Somewhat likely	8%	26%	25%	7%	25%	32%	26%
Unlikely	8%	13%	18%	31%	12%	13%	17%
Never	12%	4%	3%	10%	4%	7%	3%
Total	100%	100%	100%	100%	100%	100%	100%

Free social messaging

Please check the information you are willing to share in a social messaging utility.

	BZ	CH	DE	RF	SG	SW	US
Name	52%	14%	20%	33%	38%	23%	53%
Address	29%	10%	3%	7%	11%	8%	37%
Telephone	20%	1%	8%	7%	9%	1%	29%
Gender	37%	45%	31%	30%	41%	29%	46%
Physical location	6%	2%	0%	0%	12%	2%	22%
Names of friends and family members	21%	27%	6%	17%	37%	5%	28%
Location of friends and family members	19%	5%	6%	2%	4%	2%	24%
Hobbies and interests	64%	48%	64%	46%	44%	48%	60%
Physical characteristics such as weight, height	17%	22%	14%	27%	21%	8%	34%
Education background	40%	12%	23%	42%	15%	27%	43%
Recent purchases	39%	21%	33%	22%	17%	30%	42%
Photo & video	15%	14%	18%	32%	16%	11%	54%
Political views	31%	10%	50%	22%	21%	43%	46%
Religion	49%	12%	17%	25%	9%	21%	19%
Race	18%	32%	36%	53%	23%	41%	32%

Free social messaging

(continued)

	BZ	CH	DE	RF	SG	SW	US
Ethnicity	24%	39%	36%	52%	26%	40%	29%
Marital status	28%	29%	23%	34%	24%	20%	54%
Sexual preference	2%	0%	16%	8%	3%	11%	8%
Social activism	10%	2%	33%	15%	15%	37%	32%
Workplace issues	8%	11%	28%	10%	10%	32%	33%
Employer information	35%	6%	30%	13%	19%	28%	27%
Credit card or bank payment information	1%	1%	1%	2%	2%	0%	0%
Average	26%	16%	23%	23%	19%	21%	34%

Would you still consider using a social messaging utility knowing that the messages you receive may be false or manipulated?

	BZ	CH	DE	RF	SG	SW	US
Yes	52%	34%	27%	56%	26%	30%	41%
No	48%	66%	73%	44%	74%	70%	59%
Total	100%	100%	100%	100%	100%	100%	100%

Free social messaging

The following is a list of possible factors that may affect your use of this social messaging utility.
Adjacent response = increase use.

	BZ	CH	DE	RF	SG	SW	US
Social messaging connects members who share common likes, tastes and preferences.	78%	58%	58%	75%	65%	49%	71%
Social messaging provides opportunities to express opinion and views on important social and political issues.	72%	16%	53%	49%	48%	48%	73%
The social messaging service provides opportunities to unite with other members of the community.	80%	9%	44%	48%	34%	39%	71%
The social messaging service provides warnings about inclement weather conditions and other dangerous conditions	49%	61%	53%	51%	61%	55%	55%
The social messaging service provides clear disclosure about the possible risks of false or prank messages.	28%	39%	46%	12%	36%	49%	41%
The social messaging service ensures anonymity wherein the user's personal identity cannot be determined.	49%	51%	55%	47%	53%	64%	63%
The user has control over the types of messages he or she can receive.	71%	21%	68%	56%	35%	59%	67%

Free social messaging

(continued)

	BZ	CH	DE	RF	SG	SW	US
The social messaging service imposes strict authentication over who is able to join the online community.	62%	63%	50%	63%	62%	39%	53%
Members of the online community set standards of acceptable behavior.	26%	27%	49%	19%	30%	51%	39%
Members of the online community establish a governance body to hear complaints and enforce standards.	21%	47%	41%	19%	38%	39%	40%
Members of the online community establish a group to monitor for suspicious activities.	14%	52%	38%	20%	46%	35%	33%
Law enforcement (police) monitors for suspicious activities.	10%	48%	42%	15%	40%	38%	28%
Government sets regulations that require the social messaging provider to implement security.	27%	35%	35%	15%	39%	39%	34%

Free social messaging

Would you consider using a social network that contributed to social causes? Please use the following scale to indicate how likely you would be to use this Web 2.0 Internet application.

	BZ	CH	DE	RF	SG	SW	US
Very likely	29%	10%	27%	34%	10%	25%	23%
Likely	29%	10%	32%	13%	21%	32%	31%
Somewhat likely	26%	31%	28%	8%	37%	29%	27%
Unlikely	14%	37%	9%	30%	19%	10%	16%
Never	1%	12%	3%	16%	13%	5%	3%

Free social messaging

Please check the information you are willing to share in this social network community.

	BZ	CH	DE	RF	SG	SW	US
Name	50%	17%	19%	38%	37%	19%	50%
Address	28%	8%	3%	2%	16%	7%	36%
Telephone	20%	2%	4%	4%	7%	3%	26%
Gender	37%	39%	27%	31%	41%	36%	52%
Physical location	4%	6%	5%	2%	8%	0%	21%
Names of friends and family members	19%	28%	7%	13%	35%	2%	30%
Location of friends and family members	17%	4%	1%	1%	6%	0%	18%
Hobbies and interests	69%	47%	58%	45%	42%	50%	57%
Physical characteristics such as weight, height	16%	20%	11%	23%	24%	8%	35%
Education background	36%	16%	26%	39%	17%	23%	40%
Recent purchases	44%	17%	37%	24%	15%	28%	42%
Photo & video	16%	13%	19%	33%	14%	11%	49%
Political views	31%	6%	49%	23%	19%	46%	44%
Religion	49%	14%	20%	23%	10%	20%	24%
Race	19%	34%	33%	52%	24%	42%	33%

Free social messaging

(continued)

	BZ	CH	DE	RF	SG	SW	US
Ethnicity	21%	36%	35%	52%	26%	40%	31%
Marital status	30%	26%	22%	34%	24%	22%	51%
Sexual preference	3%	2%	21%	6%	4%	18%	13%
Social activism	13%	0%	34%	18%	17%	34%	36%
Workplace issues	11%	9%	28%	7%	15%	27%	33%
Employer information	34%	4%	25%	9%	21%	29%	30%
Credit card or bank payment information	0%	0%	1%	2%	1%	0%	0%
Average	26%	16%	22%	22%	19%	21%	34%

Would you still consider using a social network knowing that it creates a risk to the security of confidential data about your company?

	BZ	CH	DE	RF	SG	SW	US
Yes	50%	13%	27%	50%	16%	32%	31%
No	50%	87%	73%	50%	84%	68%	69%
Total	100%	100%	100%	100%	100%	100%	100%

Free social messaging

The following is a list of possible factors that may affect your use of this social network.
Adjacent response = increase use.

	BZ	CH	DE	RF	SG	SW	US
The social network provides access to a large body of information about social, ethical or environmental initiatives around the world.	43%	32%	53%	46%	35%	58%	47%
The social network provides opportunities for members to contribute their time and resources to initiatives that directly impact those in need.	34%	29%	58%	20%	30%	56%	53%
The social network provides opportunities for members and their organizations to quickly unite on critical issues and act as one voice before governments around the world.	47%	10%	59%	38%	25%	57%	41%
The social network provides opportunities for members and their companies to pool resources and target deserving charitable causes.	46%	17%	55%	26%	16%	53%	45%
The social network provides clear disclosure about the possible risks of sharing confidential company information.	25%	37%	47%	13%	36%	50%	45%

Free social messaging

(continued)

	BZ	CH	DE	RF	SG	SW	US
The social network ensures anonymity wherein the user's personal identity cannot be determined.	49%	51%	56%	47%	54%	63%	61%
The user has control over who sees or has access to personal information.	73%	20%	65%	53%	36%	58%	67%
The social network imposes strict authentication over who is able to join the online community.	64%	66%	52%	60%	58%	42%	52%
Members of the online community set standards of acceptable behavior.	24%	31%	50%	20%	33%	52%	38%
Members of the online community establish a governance body to hear complaints and enforce standards.	20%	46%	41%	18%	35%	38%	40%
Members of the online community establish a group to monitor for suspicious activities.	14%	55%	39%	21%	47%	37%	37%
Law enforcement (police) monitors online community for suspicious activities.	10%	48%	41%	16%	40%	39%	27%
Government sets regulations that require the social network to implement security.	26%	39%	35%	13%	42%	37%	38%

Wiki in the workplace

Would you consider using a wiki that enables you to share information about yourself and your work? Please use the following scale to indicate how likely you would be to use this Web 2.0 Internet application.

	BZ	CH	DE	RF	SG	SW	US
Very likely	28%	8%	25%	21%	8%	25%	23%
Likely	28%	12%	29%	10%	18%	28%	24%
Somewhat likely	22%	32%	28%	5%	37%	28%	21%
Unlikely	12%	34%	8%	29%	20%	8%	13%
Never	9%	13%	9%	35%	17%	11%	19%

Wiki in the workplace

Please check the information you are willing to share in a company's wiki.

	BZ	CH	DE	RF	SG	SW	US
Name	52%	18%	19%	37%	37%	20%	49%
Address	29%	9%	2%	3%	15%	6%	37%
Telephone	19%	2%	6%	3%	7%	2%	26%
Gender	37%	42%	29%	33%	42%	35%	50%
Physical location	5%	5%	2%	2%	9%	0%	24%
Names of friends and family members	21%	28%	7%	14%	34%	3%	32%
Location of friends and family members	19%	4%	2%	0%	5%	0%	19%
Hobbies and interests	67%	47%	60%	46%	42%	49%	59%
Physical characteristics such as weight, height	16%	21%	11%	24%	24%	9%	33%
Education background	35%	14%	25%	38%	16%	25%	40%
Recent purchases	43%	18%	36%	23%	16%	27%	43%
Photo & video	15%	14%	19%	34%	14%	12%	49%
Political views	31%	8%	47%	25%	18%	45%	44%
Religion	49%	13%	20%	24%	10%	21%	22%
Race	20%	34%	34%	54%	24%	41%	32%

Wiki in the workplace

(continued)

	BZ	CH	DE	RF	SG	SW	US
Ethnicity	22%	38%	33%	51%	27%	41%	30%
Marital status	29%	25%	23%	34%	25%	21%	53%
Sexual preference	2%	0%	21%	6%	3%	18%	11%
Social activism	13%	0%	34%	16%	18%	36%	36%
Workplace issues	10%	11%	28%	8%	14%	26%	34%
Employer information	31%	4%	27%	11%	19%	29%	32%
Credit card or bank payment information	1%	0%	1%	2%	0%	0%	0%
Average	26%	16%	22%	22%	19%	21%	34%

Would you still consider using a wiki knowing that some of uncensored content about you may be posted?

	BZ	CH	DE	RF	SG	SW	US
Yes	33%	31%	25%	37%	38%	20%	40%
No	67%	69%	75%	63%	62%	80%	60%
Total	100%	100%	100%	100%	100%	100%	100%

Wiki in the workplace

The following is a list of possible factors that may affect your use of this wiki.
Adjacent response = increase use.

	BZ	CH	DE	RF	SG	SW	US
The wiki provides relevant and timely information about the organization.	66%	43%	63%	59%	46%	69%	51%
The wiki provides opportunities for employees to organize and unite on critical issues.	48%	4%	56%	49%	18%	57%	40%
The wiki provides an opportunity for employees to maintain contact with others who share a common set of values, interests and preferences.	59%	21%	51%	41%	26%	68%	62%
The wiki provides opportunities to freely communicate issues and concerns with the organization's management.	53%	5%	58%	17%	25%	59%	40%
The company provides clear disclosure about posting content that may make others feel uncomfortable.	22%	14%	44%	20%	18%	40%	43%
The company ensures anonymity wherein the employee's identity cannot be determined when he or she posts content to the wiki.	49%	50%	59%	50%	54%	62%	59%

Wiki in the workplace

(continued)

	BZ	CH	DE	RF	SG	SW	US
The company implements strict authentication over who is able to post content to the wiki.	60%	71%	50%	63%	57%	43%	52%
The company sets standards about the posting of business information.	24%	33%	50%	20%	37%	57%	39%
The company censors all content before posting to the wiki.	10%	47%	40%	14%	40%	38%	25%
Employees have the ability to control, modify or delete any content that identifies them.	77%	20%	65%	50%	36%	55%	69%
The community of wiki users set standards of acceptable behavior.	25%	30%	53%	20%	35%	52%	36%
The community of wiki users establishes a governance body to hear complaints and enforce standards.	19%	48%	43%	15%	33%	38%	38%
The community of wiki users establishes an employee group to censor content before posting.	16%	55%	39%	22%	49%	39%	38%
Government sets regulations that restrict companies from using wikis that may reveal an employee's personal information.	16%	39%	31%	10%	45%	39%	40%
Average	39%	34%	50%	32%	37%	51%	45%

Other questions

Why would you participate in Web 2.0 applications? Please select only one choice.

	BZ	CH	DE	RF	SG	SW	US
The benefits from participating outweighs any privacy or security risk.	39%	10%	17%	44%	13%	24%	34%
I benefit from exchanging information about myself with other like-minded community members.	17%	30%	44%	24%	28%	40%	48%
I believe the security of the Web 2.0 application is adequate in protecting my personal information.	21%	49%	7%	18%	49%	7%	11%
I am aware of potential dangers and willing to take steps to protect myself.	22%	10%	33%	15%	9%	30%	8%
Other	1%	1%	0%	0%	1%	0%	0%

Do you believe the online community should take steps to protect its members?

	BZ	CH	DE	RF	SG	SW	US
Yes	74%	73%	81%	57%	74%	76%	80%
No	26%	27%	19%	43%	26%	24%	20%

Other questions

If yes, how would this work? Please check what you believe to be the most important steps the community could take. Please check the top two choices.

	BZ	CH	DE	RF	SG	SW	US
Set a code or standards that specify(ies) acceptable behaviors.	34%	12%	37%	23%	19%	57%	23%
Educate members about how to avoid potential harms.	19%	24%	34%	26%	31%	37%	18%
Enforce compliance with acceptable standards of behavior.	50%	34%	30%	53%	26%	23%	37%
Implement security tools to detect and prevent undesirable behavior.	46%	35%	54%	20%	40%	19%	44%
Demand social network provider to have better safeguards in place.	15%	16%	11%	13%	10%	26%	23%
Monitor online activities to detect threats.	21%	26%	23%	45%	25%	16%	20%
Work with law enforcement to police Web site for suspicious activity.	15%	49%	10%	18%	46%	16%	33%

Other questions

In your opinion, how can the online community be most effective in protecting its members? Please select only one choice.

	BZ	CH	DE	RF	SG	SW	US
Educating members	9%	39%	25%	6%	45%	22%	11%
Creating standards	24%	13%	9%	18%	10%	10%	23%
Monitoring standards	13%	11%	12%	9%	10%	12%	13%
Enforcing standards	14%	16%	12%	11%	12%	12%	13%
All of the above	41%	21%	42%	56%	23%	43%	40%

Other questions

Are you willing to spend time, money or other resources to advance safety and security in online communities you participate in?

	BZ	CH	DE	RF	SG	SW	US
Yes	41%	52%	68%	38%	51%	70%	55%
No	59%	48%	32%	62%	49%	30%	45%
Total	100%	100%	100%	100%	100%	100%	100%

Who do you believe is most responsible for ensuring a safe Internet? Please rank the following list from 1 = most responsible to 5 = least responsible.

	BZ	CH	DE	RF	SG	SW	US
Individual users	2.10	3.74	3.90	2.08	3.34	3.82	2.03
The online community as a whole	3.50	3.13	2.76	3.15	3.43	2.78	2.99
Internet service provider	4.32	3.96	4.04	4.25	3.95	4.42	4.21
Law enforcement	4.10	3.55	3.16	4.25	3.39	3.33	4.56
Government	3.71	2.22	2.55	3.44	3.18	2.79	3.42

Other questions

What are you willing to do in order to ensure online safety and security? Please check the top two choices.

	BZ	CH	DE	RF	SG	SW	US
Avoid high-risk Web sites	69%	35%	52%	74%	41%	46%	57%
Use and frequently change complex passwords	28%	5%	16%	33%	5%	13%	29%
Implement computer security software tools	10%	15%	25%	13%	21%	26%	18%
Thoroughly read online privacy policies	3%	4%	9%	2%	6%	10%	4%
Discontinue using suspicious Web sites	27%	23%	23%	17%	22%	23%	22%
Prevent others from using my computer	3%	36%	10%	21%	26%	16%	2%
Participate in online community security activities	2%	3%	5%	0%	4%	6%	1%
Other	1%	0%	0%	0%	1%	0%	0%
Total	143%	121%	140%	160%	126%	140%	133%

Other questions

When is online security most important to you? Please check all that apply.

	BZ	CH	DE	RF	SG	SW	US
Performing search	10%	37%	14%	21%	12%	16%	13%
Obtaining news and information	13%	44%	7%	19%	12%	10%	27%
Participating in a social network	19%	13%	22%	14%	15%	24%	20%
Using social messaging tools	6%	4%	4%	4%	3%	8%	7%
Blogging or contributing to wikis	9%	10%	8%	10%	9%	11%	5%
Browsing or shopping	28%	30%	36%	26%	40%	35%	19%
Banking or paying bills	4%	0%	3%	0%	4%	5%	11%
Sending e-mails	22%	23%	13%	10%	10%	11%	16%
Other	0%	1%	0%	0%	0%	1%	1%

Other questions

Does your organization mandate the use of Web 2.0 tools in the workplace?

	BZ	CH	DE	RF	SG	SW	US
Yes	11%	5%	18%	9%	8%	20%	24%
No	89%	95%	82%	91%	92%	80%	76%
Total	100%	100%	100%	100%	100%	100%	100%

If yes, how do you feel about having to use Web 2.0 tools? Please select best answer.

	BZ	CH	DE	RF	SG	SW	US
It is okay because it makes me more productive and efficient.	74%	50%	49%	54%	63%	51%	80%
It is okay because it is fun to use.	5%	10%	8%	5%	11%	6%	5%
It makes no difference in my ability to do my job.	11%	25%	11%	26%	18%	12%	10%
It detracts from my productivity because it is irrelevant to my job.	10%	15%	32%	15%	8%	31%	5%
Total	100%	100%	100%	100%	100%	100%	100%

Demographics

What are your primary sources for local, national and world news?

	BZ	CH	DE	RF	SG	SW	US
Newspaper (print)	38%	36%	34%	41%	40%	32%	28%
Television	34%	24%	32%	30%	25%	31%	37%
News Web sites	6%	5%	9%	10%	6%	11%	15%
Online blogs	19%	4%	12%	10%	8%	12%	11%
None of the above	3%	31%	14%	9%	22%	14%	9%

How many hours each week do you spend using the Web or doing e-mail?

	BZ	CH	DE	RF	SG	SW	US
1 hour or less	3%	15%	8%	6%	7%	6%	3%
1 to 5 hours	6%	26%	10%	13%	11%	10%	8%
5 to 10 hours	19%	15%	7%	27%	20%	9%	12%
15 to 20 hours	28%	24%	19%	13%	24%	18%	26%
20 to 40 hours	32%	15%	28%	26%	24%	33%	25%
More than 40 hours	12%	5%	27%	15%	13%	24%	26%
Median extrapolated hours	22	13	25	19	19	25	25

Demographics

What is your highest level of education attained?

	BZ	CH	DE	RF	SG	SW	US
High School	26%	27%	17%	18%	20%	20%	28%
Vocational	20%	36%	34%	28%	33%	26%	22%
University or College	42%	24%	36%	39%	38%	40%	41%
Post Graduate	11%	8%	12%	12%	7%	10%	8%
Doctorate	1%	4%	2%	3%	2%	3%	1%

Demographics

Please check your age range.

	BZ	CH	DE	RF	SG	SW	US
18 to 25	30%	21%	23%	23%	20%	22%	24%
26 to 35	16%	23%	25%	24%	24%	26%	21%
36 to 45	15%	14%	16%	15%	16%	15%	19%
46 to 55	20%	23%	19%	21%	22%	20%	18%
56 to 65	14%	11%	9%	11%	12%	10%	12%
66 to 75	1%	6%	6%	5%	5%	5%	6%
75+	4%	2%	2%	1%	1%	2%	0%
Total	100%	100%	100%	100%	100%	100%	100%
Median extrapolated age	37	39	38	39	39	38	39

Gender

	BZ	CH	DE	RF	SG	SW	US
Female	43%	36%	50%	40%	39%	53%	52%
Male	57%	64%	50%	60%	61%	47%	48%
Total	100%	100%	100%	100%	100%	100%	100%