McAfee

Web 2.0
A Complex Balancing Act

The First Global Study on Web 2.0 Usage, Risks and Best Practices

Web 2.0: A Complex Balancing Act

The First Global Study on Web 2.0 Usage, Risks and Best Practices

CONTENTS

Executive Summary 3

Introduction 4

Web 2.0 Adoption in Organizations 5

Employee Use of Web 2.0 10

Balancing Act 18

Conclusion 24

Appendices 26

Executive Summary

What are Web 2.0's leading trends in business? Defined broadly as consumer social media applications such as Facebook, Twitter and YouTube, and specialized Enterprise 2.0 solutions, Web 2.0 has become a term surrounded by many debates: To adopt or not? How can organizations use Web 2.0 technologies? What are the business benefits? Will Web 2.0 use increase or decrease employee productivity? Is the security risk worth the benefits?

In collaboration with experts in the fields of security and social media, McAfee took a close look at these questions. Commissioned by McAfee, Professors Mihaela Vorvoreanu and Lorraine Kisselburgh from Purdue University and the Center for Education and Research in Information Assurance and Security (CERIAS) undertook extensive research with experts from around the globe.

International research firm Vanson Bourne surveyed more than 1,000 organizational decision-makers in 17 countries worldwide, and combined with expert interviews, we developed an in-depth study of emerging policies and practices into how organizations balance the risks and benefits of using Web 2.0 technologies.

Our findings show high Web 2.0 adoption. Three out of four organizations worldwide use Web 2.0 for a variety of business functions such as IT (51 percent), marketing and sales (34 percent), customer relations (29 percent), advertising and public relations (28 percent) and human resources (22 percent). The main driver for Web 2.0 adoption is new revenue potential, according to two thirds of our respondents. Only 42 percent of those surveyed felt strongly about the importance of present Web 2.0 tools. While organizations acknowledge revenue potential and business value in Web 2.0 technologies, leaders and decision makers debate employee use of Web 2.0 in the workplace — either in the office or on the road.

Security is the leading issue. Half of the organizations say it is their primary concern for Web 2.0 technologies. For another third, security is the main reason they don't use Web 2.0 more widely. Six out of 10 organizations suffered large losses averaging $2 million each because of security incidents during the past year. Together, more than $1.1 billion was lost by these organizations due to security incidents.

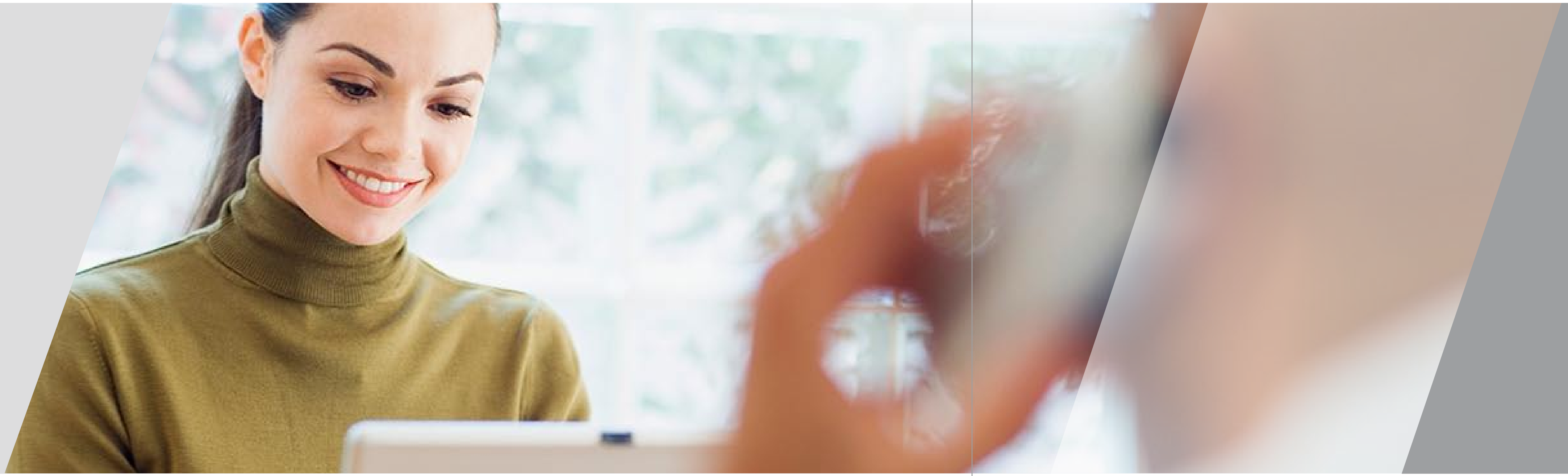
One of the main sources of security threats is employee use of social media. Thirty-three percent of organizations worldwide restrict employee use of it; 25 percent monitor use; and 13 percent block all social media access. Social network sites are regarded as the main security threat of all social media tools. As a result, nearly half of the organizations we surveyed block Facebook.

Organizations need to employ a variety of measures to ensure safe use of Web 2.0. Social media policies and technological protection are the two primary measures used today. Two thirds of organizations worldwide have social media policies for employees, and 71 percent of those use technology to enforce them. However, that leaves one third of organizations without a social media policy, and almost half of the organizations lack a policy for Web 2.0 use on mobile devices.

To address these challenges, many organizations have increased security protection since introducing Web 2.0 applications. Seventy-nine percent increased firewall protection, 58 percent introduced greater levels of web filtering, and 53 percent implemented greater web gateway protection. Two out of five organizations are budgeting for Web 2.0-specific security solutions.

Security experts strongly recommend a multi-layer security approach that's customized for Web 2.0-specific challenges to mitigate adoption risks. Eugene Spafford, founder and Executive Director of CERIAS at Purdue University, notes that "the best protections are those that don't get in the way of getting work finished, because users are not tempted to circumvent those controls. As not all information needs to be protected in the same way, and not all users are going to interact with Web 2.0 technologies in the same manner, defenses should be tailored to fit the circumstances of use."

Executives and industry experts agree that successful organizational use of Web 2.0 is a complex balancing act. It requires analyzing challenges and opportunities while mitigating risks, and combining policy, employee training and technology solutions to ensure security.



“By 2014, social networking services will replace e-mail as the primary vehicle for interpersonal communications for 20 percent of business users.” [Gartner (2010). “Predicts 2010: Social Software Is an Enterprise Reality.”]

Introduction

Web 2.0 — defined here broadly as consumer social media applications such as Facebook, Twitter and YouTube, and specialized Enterprise 2.0 solutions — has become a term surrounded by many debates: To adopt or not? How can organizations use Web 2.0 technologies? What are the business benefits? Will Web 2.0 use increase or decrease employee productivity? Is the security risk worth the benefits?

McAfee, in collaboration with communication media and IT security experts, and with the help of international research firm Vanson Bourne, investigated these questions. A survey of more than 1,000 organizational decision makers from 17 countries, and in-depth interviews with experts, paint a complex picture with two main Web 2.0 issues: the opportunities provided to organizations that have adopted Web 2.0, and the challenges of embracing emerging technologies at infrastructure and employee levels. In balancing these challenges and opportunities, the report discusses measures organizations take to ensure safe use of Web 2.0. The survey data and expert opinions corroborate that while Web 2.0 has considerable value, using Web 2.0 applications successfully is a balancing act that requires a combination of technology, policy and education.

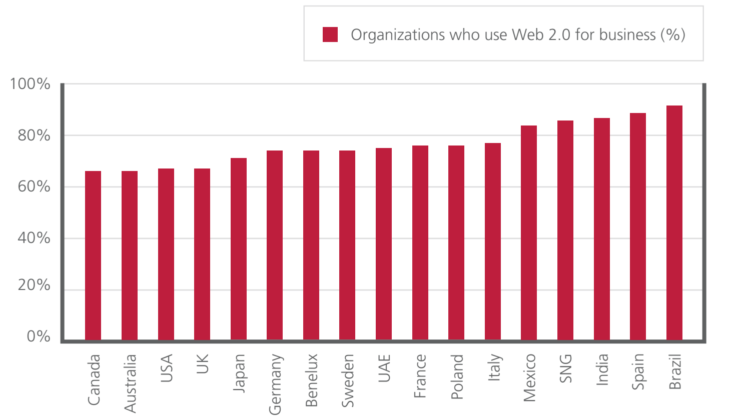
Web 2.0 Adoption in Organizations

Our survey shows high adoption of Web 2.0 in the enterprise. More than 75 percent of organizations reported using Web 2.0 solutions for many business functions. While adoption rates vary across countries, they were high overall, and reached 90 percent or higher in Brazil, Spain and India. Web 2.0 adoption was lowest in the United States and the Commonwealth countries of the United Kingdom, Australia, and Canada.

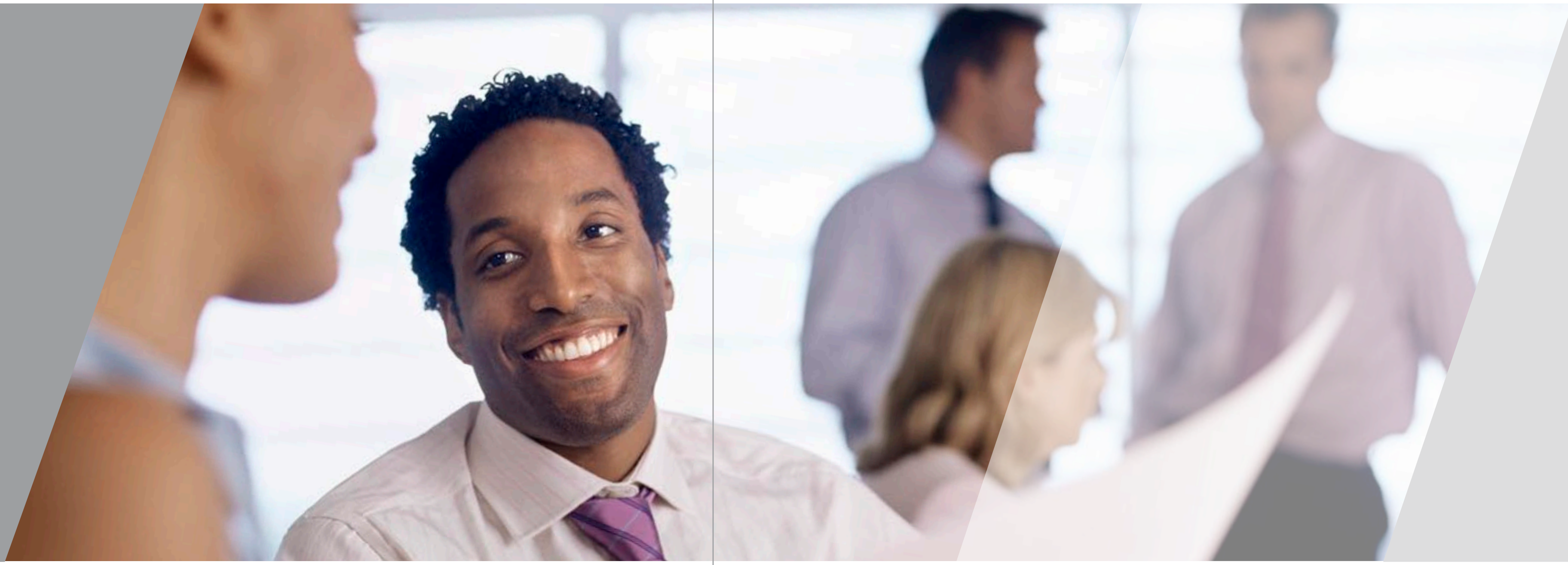
Survey data confirmed market research group Gartner’s anticipated trend: “By 2014, social networking services will replace e-mail as the primary vehicle for interpersonal communications for 20 percent of business users.” [Gartner (2010). “Predicts 2010: Social Software Is an Enterprise Reality.”]

Web 2.0 solutions are used for a variety of business purposes. About half of the organizations surveyed employ Web 2.0 solutions for IT functions, and roughly a third of organizations use them for marketing, sales or customer service. One in five organizations reported using Web 2.0 for public relations or human resources — especially recruitment. India leads in adoption of Web 2.0 for IT solutions, with about three out of four Indian organizations reporting such use.

Web 2.0 Adoption Rates by Country



Crowd-sourcing is one of the ways that companies are leveraging Web 2.0 to create new revenue streams. InnoCentive is an online crowd-sourcing company where organizations as large as Eli Lilly, DuPont, Boeing, Procter&Gamble and NASA post research problems in need of solutions. Scientists from all over the world, whether amateur, professional, or retired, choose problems to work on and post their solutions. Companies select a winning solution and pay the scientist a cash prize ranging from $5,000 to $1 million, depending on the problem's complexity. InnoCentive enables companies to solve difficult research problems at a much lower cost than their own R&D departments, and to have access to a diversity of solutions, ideas and expertise that is unlikely to occur within just one organization. http://www2.innocentive.com



New revenue streams emerged as the highest driver of Web 2.0 adoption. Three out of four organizations that use Web 2.0 reported that expanded use of Web 2.0 technologies could create new revenue streams for their organizations. This is especially true in Brazil, India, the United Arab Emirates and Mexico, where nine out of 10 organizations share this belief. Even 65 percent of organizations in the public sector that already use Web 2.0 see revenue potential from using it. However, perceived importance of Web 2.0 solutions was tempered. Forty-two percent of respondents who reported using Web 2.0 solutions agreed they were important to business, but about the same percentage was neutral.

Three out of four organizations that use Web 2.0 reported that expanded use of Web 2.0 technologies could create new revenue streams for their organizations.

Frank Gruber, co-founder of TECH cocktail, discusses some of the ways that companies are leveraging Web 2.0 technologies — and particularly the people participating in these platforms — to facilitate production, marketing, and customer service:

"For example, crowdsourcing has been used for design work, solving difficult problems and even to make product decisions. There are a number of companies leveraging Web 2.0 technologies for social media marketing campaigns and for customer service. Ford has been leveraging social media and outreach to connect with a newly invigorated Ford Fiesta. Zappos leverages Web 2.0 for customer service, because every employee has a Twitter account for customer support and feedback. Intel works with bloggers to spread the word about their innovations."

Market pressure was not, overall, a big driver of Web 2.0 adoption. The exception is India and Brazil where 78 and 58 percent, respectively, reported that customers and partners are requesting organizations to engage in Web 2.0. Perceived market pressure was higher in the public sector, where almost half of organizations feel it, as opposed to only a third in the private sector. In the largest organizations, the pressure to engage in Web 2.0 offerings was highest. Almost half of large organizations reported partner or customer demand, compared to only a third of small organizations.

The survey data suggests that in 2010 Web 2.0 solutions are not perceived as crucial to organizations.

The survey data suggests that in 2010 Web 2.0 solutions are not perceived as crucial to organizations. This is not surprising, given that some of the technologies have not reached maturation, and uses are still being explored. However, respondents see great potential for Web 2.0 in the future, and the data suggests that this belief drives adoption. Stowe Boyd, analyst and business strategist, claims the real benefits of Web 2.0 become apparent when adoption rates reach 90 percent. "The more people use social tools, the more efficient the tools become," states Boyd.

In addition to supporting communication and collaboration among employees, organizations recognize the value Web 2.0 technologies bring to clients and customer relations. About 40 to 45 percent of organizations feel that Web 2.0 improves customer service, and 40 percent feel it enhances effective marketing.

"The more people use social tools, the more efficient the tools become."

Although Web 2.0 was not considered extremely critical for many organizations in this study, for one organization it is vital. *charity: water* is a nonprofit organization that provides clean and safe drinking water in the developing world. It directs 100 percent of public donations to funding water projects. *charity: water* does nearly all of its fundraising online and has no budget for marketing or advertising. *charity: water* has raised more than $7.5 million in its first two years of operation using mainly an online community platform and social media. With the power of social media alone, in 2009 more than $250,000 was raised in a single day when *charity: water* was the beneficiary of Twestival Global. This resulted in more than 55 water wells in Uganda, Ethiopia and India, and touched the lives of an estimated 17,000 people. "Web 2.0 is the heart of our operation and our primary source of revenue. We're a Web 2.0 charity," says *charity:water* director of digital engagement, Paull Young. *charity:water* is a convincing example of the impact social media can have on ROI.

McAfee CTO and vice president, Raj Samani, believes that more companies should be concerned about security. He explains that the security landscape has changed. Whereas 10 to 15 years ago data infiltration was the biggest concern, these days data exfiltration, good data going out, is the primary challenge. In an economy where information is the lifeblood of an organization, preserving the confidentiality, integrity and availability of information is vital. Virus and malware protection is still important, but data loss prevention is fast becoming an indispensable component of an organization's technology protection.

If Web 2.0 is useful for business functions, what is preventing organizations from using it more? Security is the leading concern for Web 2.0 technologies. Half of the respondents name security risks as their primary concern with Web 2.0, while a third identify fear of security issues as the main reason Web 2.0 applications are not used more widely in their business. Trepidation about security is higher than average in India and Brazil, two countries with the highest Web 2.0 adoption rates. Large organizations are twice as likely as small organizations to avoid using Web 2.0 because of security fears. With more employees and more complex infrastructures to protect, it is no surprise that large organizations perceive higher risks. At the same time, large organizations report the highest benefit from using Web 2.0 tools such as collaborative platforms.

Fears and concerns about security are well founded. Six out of 10 organizations experienced some sort of security incident the previous year because of Web 2.0 technologies — virus and malware infections were the most common. The financial loss associated with these security incidents was high. On average, organizations lost almost $2 million the previous year because of security incidents.

Large organizations paid even steeper costs for security breaches because of Web 2.0 usage. The average loss for a large organization was $4.5 million, with an average reported loss around $10 million in Japan and Singapore, and more than $8.5 million in Canada. Large organizations in the United States have managed their security risks better, and reported a relatively lower average loss of $1.7 million.

Organizations in countries with high Web 2.0 adoption such as Brazil, India and Mexico were most likely to have experienced security incidents and to report large losses. The average amount lost by Brazilian organizations was $2.5 million. Japan reported the highest average loss per organization at $3 million. Organizations in the United States lost, on average, more than $1.5 million due to security breaches.

Six out of 10 organizations experienced some sort of security incident the previous year because of Web 2.0 technologies — virus and malware infections were the most common.

What accounts for Brazil's high Web 2.0 adoption rate? Brazilian IT consultant and ICANN member, Vanda Scartezini, explains that Brazilians tend to love novelty and are quick to adopt new technologies. At the same time, Brazil is seeing "huge infection problems" originating from social media. Scartezini recommends that organizations use more than one security software applications to protect assets.

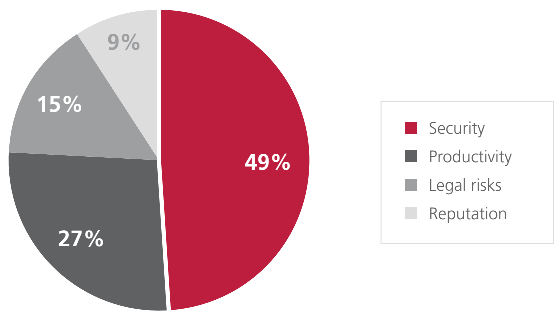
Virus and malware infections are the most common types of security incidents. A third of organizations experienced virus infections and almost a quarter experienced malware infections the previous year. In spite of concerns about data exfiltration, very few organizations (less than one in 10) reported experiencing data leaks or information overexposure. Security experts found this percentage to be lower than expected, and explain that respondents might be aware of or report only the more serious incidents. Pamela Warren, McAfee cybercrime strategist, stated, "more data leaks might have happened, but they are outside organizations' awareness."

Beyond security, other factors that account for limited use of Web 2.0 in organizations include lack of demand and lack of applicability, reported by 18 percent of respondents. Lack of productivity and legal risks also emerged as Web 2.0 concerns. However, these reasons lag far behind security fears.

Despite high adoption rates and strong business benefits, concern over security remains the leading factor holding organizations back from exploring the full potential of Web 2.0 applications. The cost and risk of security incidents are very high. A large proportion of security fears are related to employee use of social media, both for work and personal purposes.

More than $1.1 billion was lost by organizations surveyed due to security incidents caused by Web 2.0 technologies.

Primary concern about Web 2.0



Employee Use of Web 2.0

While organizations see revenue potential and business value in Web 2.0 technologies, decision makers continue to debate whether or not to allow employee usage of Web 2.0 in the workplace — either in the office or on the road.

Some organizations emphasize education, guidelines and usage policies that provide parameters for appropriate and allowable use of Web 2.0 technologies for work. In other cases, organizations are responding to rising employee and customer demand for making Web 2.0 technologies available, and are less concerned about employee productivity or security threats.

But many organizational leaders are highly concerned with potential threats from Web 2.0 technologies. They worry about security, data integrity, employee productivity, along with the reputational, financial, legal and technological consequences that can occur as a result of Web 2.0 usage.

In spite of these concerns, 29 percent of organizations do not have policies regarding employee usage of Web 2.0 in the office, and fewer still have policies in private sector and small organizations. Seventy-five percent of organizations without policies indicate they trust their employees to use tools appropriately, or do not consider social media a threat.

Many organizations that do not restrict employee usage report positive results from social media tools including enhanced communication and increased employee productivity. Most organizations rated webmail and collaborative platforms as the most useful applications. Only a quarter of organizations rated social network sites and streaming media sites such as YouTube as useful.

Perceptions of Web 2.0 Utility for Employee Use

WEB 2.0 TOOL	RATED USEFUL BY ORGANIZATIONS	PROVIDED BY ORGANIZATIONS
WEBMAIL	48%	90%
COLLABORATIVE PLATFORMS	42%	82%
CONTENT SHARING APPLICATIONS	40%	86%
STREAMING MEDIA SITES	28%	82%
SOCIAL NETWORK SITES	25%	77%

Seventy-five percent of organizations without policies indicate they trust their employees to use tools appropriately, or do not consider social media a threat.

While Web 2.0 tools were most likely to be considered useful for improving communication, survey respondents also reported other benefits: enhanced customer service, increased productivity, as well as marketing and branding. For example, half of respondents reported that use of collaborative platforms improves productivity. Forty-two percent of respondents said social network sites enhance customer service.

Organizational leaders differed, however, on whether they felt Web 2.0 increased employee productivity. Only 40 percent of organizations agreed that Web 2.0 tools enhance productivity. However, organizations are more likely to indicate that collaborative platform and content sharing applications are more useful for productivity than streaming media and social networking tools. The social nature of these tools may factor into the reluctance of organizational leaders to embrace adoption, as well as their relative novelty in the organization.

Analyst and business strategist, Stowe Boyd, discusses the historical resistance to emerging technologies in organizations. "When American businesses after WWII started to think about rolling out telephones on everyone's desks, the biggest objection that was raised by the senior managers, who already had telephones, was that everyone was going to use these phones for personal use. They were going to call mom; they were going to gossip. They weren't going to use them primarily to do business. But [most of the] time, business people use telephones to conduct business because it's an efficient, and direct and obvious way to do it. The exact same thing happened with e-mail, the exact same thing happened with instant messaging, and now with social media, especially the stuff that has social networks in it, they are saying exactly the same stuff. 'We've got to manage this because they're going to be sitting there talking about fantasy football.'"

Mobile social media access can be life saving during large-scale natural disaster emergencies, and played a major role in relief and recovery efforts during the 2010 Haiti earthquake. Twitter and Facebook were critical to communicating information about relief efforts. Shortly following the earthquake, the U.S. State Department began posting assistance information on its Facebook page.

Agencies, such as the American Red Cross, and citizens used Twitter to provide minute-by-minute status changes on the ground, and to mediate communication with those outside the disaster zone to assist in relief efforts. Volunteers used mobile GPS and camera-enabled phones to gather photographic and geographic data about roads, buildings and people. The information was posted to a collective Google Maps mashup that allowed emergency personnel to locate open roads for relief transportation, and identify "last-seen" locations of individuals seeking family. Building a social media following during quiet times ensures your message gets across quickly and credibly during a crisis, even if conventional lines of communication are down.
http://fcw.com/articles/2010/01/14/social-media-haiti-earthquake-relief.aspx
http://www.readwriteweb.com/archives/social_media_red_cross_floods.php

Only 40 percent of organizations agreed that Web 2.0 tools enhance productivity.

GE has used internal Web 2.0 collaboration tools for many years now. As a large multinational corporation with a workforce scattered all around the world, GE needed online collaboration and social tools. By now, "people have gotten so used to them that they've come to depend on them," says GE systems engineer Anthony Maiello. GE is going beyond your out-of-the box internal social networking solution: "Those are great for communication, but they do not meet our specialized design needs," explains Maiello. GE is building sophisticated collaboration tools that enable engineers to collaborate remotely and create complex technical designs. "Because new products are being created on this platform, security is a paramount concern. We do not want external parties attacking our network and getting to this information," says Maiello.

Jonathan Grudin of Microsoft Research, who studies computer-supported cooperative work, notes that concerns about emerging technologies encroaching on employee productivity are not new. It took many organizations about 15 years before accepting e-mail technologies because "they had the same concerns about confidentiality and productivity. There were leading industry analysts and organizational behavioral theoreticians who claimed in the 1990s that e-mail was actually a productivity killer. However, when reliable attachment features were added to e-mail systems, allowing documents, spreadsheets and slide decks to be e-mailed, "managers saw the value, and then it became mission critical." Similarly, Grudin adds, a decade ago, "company executives warned against IM use in the company, claiming again that it was a productivity killer, and it too is now seen as mission critical in many organizations. So there is a history of organizations raising concerns about informal modes of communication."

In fact, an increasingly mobile workforce has made information and communicative technologies essential to communication as well as productivity in organizations. Disaster and crisis situations provide a compelling argument for employee use of social media — mobile technologies facilitate communication when traditional infrastructures fail. When the U.S. Naval base in Millington, Tenn., flooded in 2010, 300 residents were displaced and their mobile phones were their only connection to the world. The U.S. Navy used Facebook to keep residents informed and help them get safely to restored buildings.

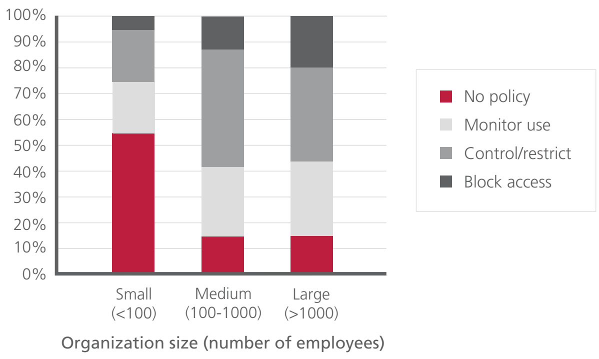
While certain organizations embrace Web 2.0 usage by employees, the majority of organizations trend differently: eighty-one percent of organizations indicated that they restrict the use of at least one Web 2.0 tool because they are concerned about security. Organizations in the United Kingdom, Germany, Canada, Sweden and Singapore are less likely than other countries to restrict use of particular tools. Larger organizations are more likely to place restrictions on social media usage than the smallest organizations (87 percent versus 67 percent, respectively).

Organizations restrict social media usage through policy, technology and controlling use of user-owned devices. More than half of organizations do not allow employees to use their own software or hardware in the workplace, and 25 percent of organizations restrict social media usage to specifically authorized individuals.

Today's workforce is likely to have access to information and communication tools at home as well as in the workplace. Ubiquitous connectivity is becoming an expectation of the 21st century, whether using consumer-owned or organizationally-provided devices. This poses an additional challenge to IT security. Indeed, more than half of organizations do not allow employees to use their own software or hardware in the workplace, and in Canada and the United Kingdom 70 percent of organizations restrict external hardware or software. We expect to see this trend decreasing in the near future, as a growing number of employees from the Millennial Generation enter the workforce and demand ubiquitous connectivity and more open policies toward consumer devices and social media.

At the most extreme, 13 percent of organizations block social media access at the infrastructure level. Blocking usage is more prevalent in the public sector and in larger organizations, where it was reported by 20 percent of organizations.

Patterns of Blocking Social Media



Eighty-one percent of organizations indicated that they restrict the use of at least one Web 2.0 tool because they are concerned about security.

General Motors, a major U.S. automobile manufacturer, empowers employees to promote their latest car models. Employees can borrow cars overnight or for the weekend and allow friends and relatives to drive them, as long as an employee is a passenger. Employees can share their experience with the car online. "Maybe they'll go onto Facebook and tell their friends, 'you know, I just drove the new Camaro and man, it's just an awesome car!'" says Holtz, who is not affiliated with GM. This program capitalizes on employees' peer groups and social networks to enhance marketing and potentially increase sales.

http://www.gm.com/corporate/responsibility/community/news/2010/plant_city_tour_030110.jsp

While IT security experts favor blocking social media if it is not applicable to an employee's job, industry analysts feel strongly otherwise. Enterprise 2.0 consultant and writer Dion Hinchcliffe thinks blocking social media is "short sighted." Consultant and writer Shel Holtz feels blocking access is "the laziest way to approach the problem," and argues that companies should "tease value out of their employees' social graph." Holtz states that employees' social connections, which they create and maintain through social media, are a great resource that organizations should capitalize on. Instead of blocking social media, Holtz believes organizations should have safe systems in place for using Web 2.0. Employees can use social media not only for marketing, but also for getting quick feedback, testing ideas and helping with recruitment. "I guarantee you your engineers know who the next best engineering hire is, because they network with other engineers and they know who has the right set of skills and knowledge and background, and who brings the right experience to the job and who would be a good cultural fit in the organization," says Holtz.

"The organization has to design for a loss of control."

While IT security experts favor blocking social media if it is not applicable to an employee's job, industry analysts feel strongly otherwise.

While blocking access to social media provides better security, these analysts agree that it is neither feasible nor sustainable in the face of emerging use in the 21st century. Instead, we're living in a future were organizations must plan and design environments with less control of employee activities. JP Rangaswami, CIO and Chief Scientist of British Telecom, recommended in a recent keynote presentation to the E2.0 2010 conference: "The organization has to design for a loss of control." Charlene Li, industry analyst and CEO of Altimeter Group, notes that "the sense of control you have to give up is significant, and executives in particular are not going to invest in something unless they know it's going to add particular value to the company." The value of Web 2.0 technologies, Li points out, comes in focusing upon the relationships that can be formed, not the technology. "It's not so much about being on Twitter as the purpose and the reason, and the connections you can form with people. It is about the human aspect of technologies, and this is nowhere more important than in using social technologies."

The primary concern that organizations have about employee usage of Web 2.0 technologies is security. This concern is a specific obstacle to adoption and integration of social media in organizations. The top four perceived threats from employee use of Web 2.0 are malicious software (35 percent), viruses (15 percent), overexposure of information (11 percent) and spyware (10 percent).

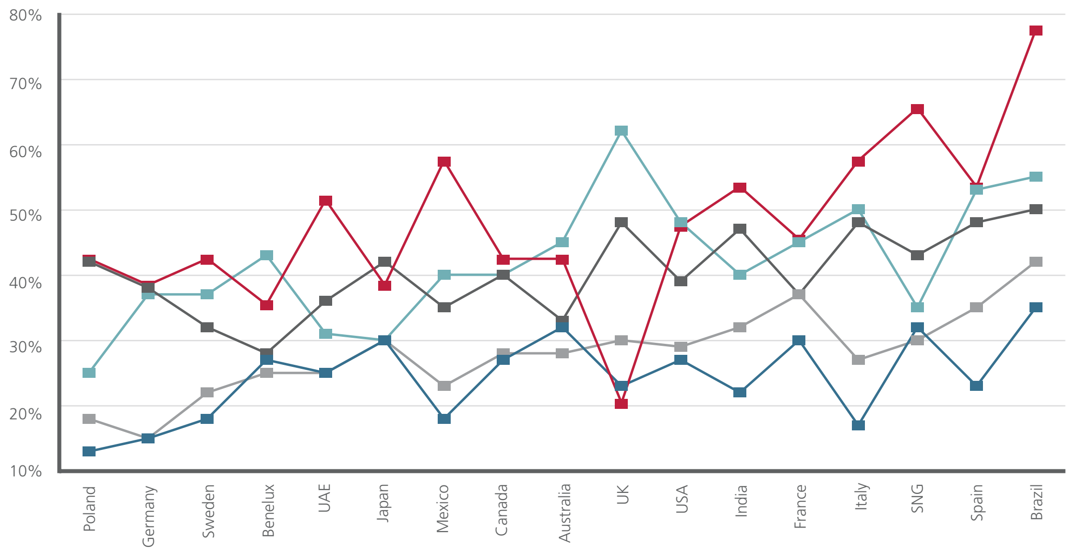
Top Perceived Security Threat from Employee Web 2.0 Usage

TOP PERCEIVED SECURITY THREAT FROM EMPLOYEE WEB 2.0 USAGE	
MALWARE INTRODUCTION	35%
VIRUS INTRODUCTION	15%
INFORMATION OVEREXPOSURE	11%
SPYWARE INCREASE	10%
SPAM VOLUME INCREASE	6%
EXPOSED ENTRY POINTS	6%
DATA LEAKS	7%
BOTNET INTRODUCTION	5%
SPAM USE INCREASE	4%

Some security concerns are specific to Web 2.0 tools used by employees. For example, technologies that are perceived to facilitate work productivity, such as webmail, collaborative platforms and content sharing applications, are less likely to raise concern than the mainstream social media tools such as Facebook, LinkedIn, YouTube and Twitter, which are not allowed by 40 to 50 percent of organizations. There are regional differences, as well, in which tools are considered useful for employees. Organizations in Brazil and Singapore, where overall adoption is high, are much more likely to rate webmail useful than organizations in the United Kingdom. However, the United Kingdom reports higher adoption of collaborative platforms and content sharing tools. Adoption of streaming media and social network sites is fairly consistent across all countries.

Industry analyst Charlene Li notes that differences in social media usage by country are less about cultural differences than about differences in access and social media penetration rates. Li says that because of high penetration rates, "South Korea and Brazil are more likely to be producing content, while other countries like the U.S. lean more towards content sharing."

Web 2.0 Applications Adoption by Country



"If it's popular, it's going to be popular with the bad guys, not just the good guys."

Facebook is banned by nearly half of the organizations, especially mid — to large-sized ones.

Social network sites are perceived as the riskiest of all Web 2.0 tools from a security standpoint.

Close to half of the leaders surveyed felt that employees are most prone to using social media inappropriately by accident, perhaps due to lack of awareness, or when they are dissatisfied with compensation or management.

One in four respondents did not have concerns about employees using social media inappropriately.

Social network sites are more likely to be linked to security issues than other technologies. Among respondents who have experienced security incidences in their organizations, half suspected social network sites as the cause, and 44 percent suspected webmail. In contrast, only 20 to 25 percent of organizations suggested content sharing and collaborative platform tools as the cause of security incidents.

These statistics suggest that many organizations perceive employee usage of Web 2.0 to be non-productive and potentially detrimental to business goals. Facebook is banned by nearly half of the organizations, especially mid — to large-sized ones. In certain European countries like Benelux, Italy and Spain, more than 60 percent of organizations restrict usage. In contrast, only a third of organizations in Japan, Germany and Brazil restrict Facebook.

Security experts explain that negative media coverage of Facebook over unilateral privacy changes might account for some of this concern. Also, the more users a tool has, the more likely it is to be a target. "If it's popular, it's going to be popular with the bad guys, not just the good guys," said an IT security professional from a major global nonprofit.

In some cases, organizations are concerned about situations that might give rise to employees inappropriately using social media. Close to half of the leaders surveyed felt that employees are most prone to using social media inappropriately by accident, perhaps due to lack of awareness, or when they are dissatisfied with compensation or management. Concerns about inappropriate usage caused by managerial disputes are higher in Spain, Brazil, Mexico and India, while pay disputes cause more concern to organizations in the United Kingdom and Australia. Concerns about accidental misuse are highest in the United Kingdom and Canada.

In contrast, one in four respondents did not have concerns about employees using social media inappropriately. Respondents from small organizations and from Sweden, Germany, Japan and the United Arab Emirates were the least likely to be concerned that employees would use social media inappropriately, where approximately 40 percent of leaders were unconcerned.

There are both real and perceived consequences of inappropriate Web 2.0 and social media use:

- The financial consequence for security incidents (including downtime, information and revenue loss) is an estimated average of $2 million for all Web 2.0 technologies.
- Sixty percent of companies report that the most significant potential consequences from inappropriate social media usage are loss of reputation, brand, or client confidence.
- One in three organizations reported unplanned investments related to "work-arounds" necessary for implementing social media in their organization.
- Fourteen percent of organizations report litigation or legal threats caused by employees disclosing confidential or sensitive information, with more than 61 percent of those threats caused by social media disclosures.

Organizational leaders are facing real consequences when adopting Web 2.0 technologies, but they recognize a growing demand for employee usage. They continue to seek the right balance to ensure technological security while embracing and integrating the opportunities presented by Web 2.0 technologies.

Legal risks are a major concern for highly regulated industries such as healthcare or financial services. One hospital system, however, found a way to use social media successfully while staying within the limits of the Health Insurance Portability and Accountability Act (HIPAA). Scott & White Healthcare is one of the largest healthcare systems in the United States, operating 10 hospitals in the Texas area. Scott & White uses Facebook, YouTube, Twitter and blogs to communicate with the public. On Nov. 5, 2009, a soldier opened fire at the Fort Hood military base in Texas, killing 13 people and wounding dozens of others (CNN, 2009). Scott & White Memorial Hospital in Temple, Texas, was the closest Level 1 trauma center and received the highest number of Fort Hood casualties. Steve Widmann, director of web services at Scott & White, used Twitter, a blog and YouTube to issue continuous updates throughout the day about access to the hospital's emergency room, hospital operation status and to keep the media and public informed. Both the local media and the public showed support and gratitude for being kept up-to-date on developments.

http://www.cnn.com/2009/CRIME/11/12/fort.hood.investigation/index.html
http://www.forimmediaterelease.biz/index.php?/weblog/comments/the_hobson_holtz_report_-_podcast_503_november_23_2009/

"We vehemently encourage every one of our clients to have a social media policy before anybody engages in social media."

Matthew Gain, Head of Digital Communications, Edelman Australia.

Balancing Act

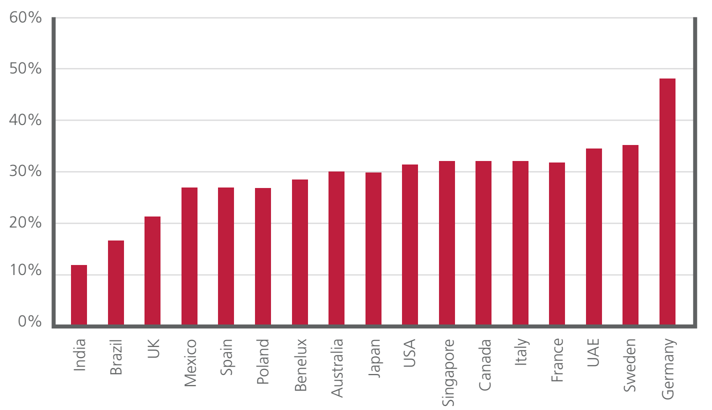
Globally, leaders of organizations agree that security concerns and issues with employee use of social media are the two major barriers for successful implementation of Web 2.0 in their organizations. In order to maximize the benefits from Web 2.0, organizations need to take measures to mitigate these risks.

Shel Holtz, consultant and writer, summarizes the balance for which organizations should strive:

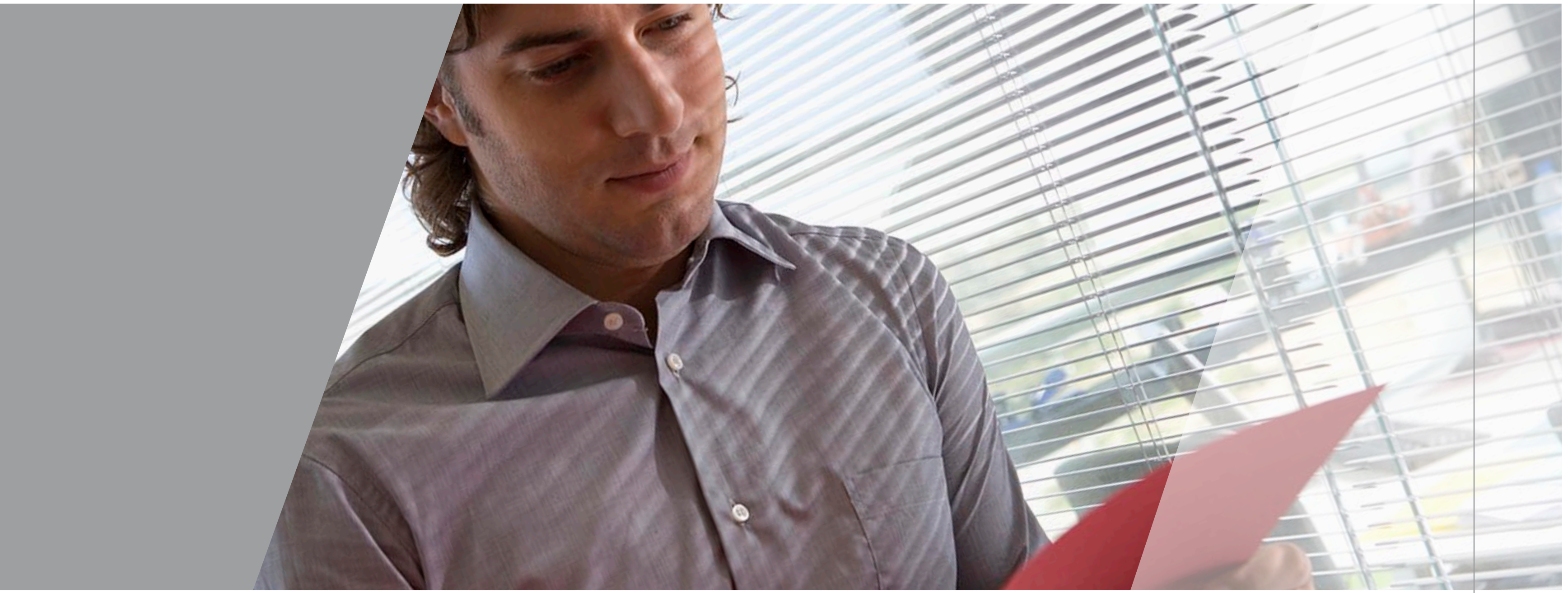
"Between shutting everybody off altogether and opening everything up to every risk possible — there's a lot of room in between those two extremes to find a balance. The balance is a combination of technical solutions and training and education. Ultimately, if you arm your employees with the knowledge they need to protect the organization's assets and engage effectively when they're talking about work and connecting from work, you're likely to experience very few of these issues. Organizations do risk benefit analyses every single day in other dimensions of business and decide that the benefit of doing something is worth the risk. I don't see why Web 2.0 should be any different. If we can, for example, reduce our customer service costs by 10 million dollars a year, by having our employees engaging through these social channels, and we calculate the risk at being one million dollars, that's a nine million dollar addition to your bottom line. And I don't know an organization that wouldn't be willing to risk a million dollars to make nine."

A third of organizations have no social media policies in place, and close to half do not have policies for social media use on mobile devices.

Organizations without social media policies



Our research indicates that risk mitigation measures most commonly include social media policy combined with protection through technology. Seventy-one percent of organizations have a workplace social media policy in place. Both security experts and industry analysts agree that social media policies are very important, although some argue that existing policies can extend to emerging contexts and channels of communication. However, a third of organizations have no social media policies in place, and close to half do not have policies for social media use on mobile devices. Both Holtz and Pamela Warren, McAfee cybercrime strategist, argue that social media policies alone are not sufficient and must be supplemented with employee education and training.



We asked organizations that do not have a social media policy in place the reasons why. Trust in employees and an unperceived threat were equally important reasons, each mentioned by more than a third of respondents. Several countries have high trust in employees. About 50 percent of respondents from Singapore, Poland and India reported trusting employees to know what is in the company's best interest. Threat perception related to social media also varies significantly across countries. Seventy percent of respondents in the United Arab Emirates, and about half of respondents from Mexico, Brazil and Sweden do not perceive any threats. However, the reported costs of recent security incidents in Mexico and Brazil suggest that social media is more of a threat than perceived by this group of respondents. Only 7 percent of organizations without social media policies reported intending to introduce them in the near future.

For the more than two thirds of surveyed organizations with social media policies in place, coverage typically includes employee liability in the case of inappropriate use, along with guidelines for approved social media sites.

Social Media Policy Coverage

TERMS OF POLICY	COVERAGE
EMPLOYEE LIABILITIES IF INAPPROPRIATE USE OCCURS	54%
GUIDELINES ON COMPANY-APPROVED SOCIAL MEDIA SITES	45%
GUIDELINES ON SECURITY ISSUES OF SOCIAL MEDIA	39%
GUIDELINES ON COMMERCIAL DANGERS OF SOCIAL MEDIA	38%
COMPANY LIABILITIES IF INAPPROPRIATE USE OCCURS	37%
GUIDELINES ON REPRESENTING THE COMPANY USING SOCIAL MEDIA	30%
ONLY CIO-AUTHORIZED STAFF USAGE ALLOWED	26%

Industry experts caution that social media policies should be enabling, not restrictive or punitive. "Most social media policies I see are bad to begin with," says Dion Hinchcliffe. "They are pages upon pages of 'though shalt not,' and by the time you're done reading, you don't know what you CAN talk about." A good policy is short and to the point — Stowe Boyd's favorite is Microsoft's "Blog smart." Hinchcliffe recommends including examples in social media policies, so that employees are exposed to a range of possible situations.

Seventy-one percent of organizations have a workplace social media policy in place.

Many organizations choose to restrict social media use for some employees, and give unlimited access to their marketing or public relations departments. For half of the organizations surveyed, social media policies varied by department, but an equal number applied the same policy to all employees. Private sector organizations, which have greater marketing needs, are more likely to vary social media policies across departments. Respondents seem to be sensitive to the fast-changing Web 2.0 landscape, and almost half of them anticipate modifying their social media policies within a year.

Industry experts agree that in addition to policy, organizations need one or more levels of technology to protect the organization and its assets. The organizations we surveyed reported using several types of technology solutions to enforce social media policies. Of the nearly three quarters that reported using technology solutions, four out of five use web filtering and firewall technology. Two thirds reported using endpoint security such as antivirus software, and 41 percent said they protect against data leakage.

Policy Enforcement Technology

	USAGE
WEB FILTERING TECHNOLOGY	83%
APPLICATIONS FIREWALL TECHNOLOGY	78%
ENDPOINT SECURITY (E.G. ANTIVIRUS)	63%
DATA LEAKAGE PROTECTION	41%

More than half of surveyed organizations have increased security measures since allowing access to Web 2.0 applications. These results suggest emerging trends in security measures that provide enhanced protection for Web 2.0 challenges. Increased firewall protection was the most commonly reported measure, but, organizations use a combination of technologies.

Implemented Security Measures Post-Web 2.0

	USAGE
INCREASED FIREWALL PROTECTION	79%
INTRODUCED GREATER LEVELS OF WEB FILTERING	58%
GREATER WEB GATEWAY PROTECTION	53%
APPLIED SITE VERIFICATION/AUTHENTICATION	31%
INTRODUCED ELECTRONIC POLICIES	27%

Web 2.0 applications are deployed "in the cloud" and accessed with desktop, laptop, and mobile devices over both wired and wireless infrastructures. This represents a challenge for security practices that have focused on endpoint and network-level infrastructure controls. Trends indicate a growing interest and implementation of web filtering and web gateway solutions in the organizations we surveyed, and roughly 55 percent of the organizations have adopted one or both of these measures since allowing access for employees.

Eugene Spafford, Executive Director of CERIAS, cautions that because the Web 2.0 technology in use is evolving quickly. It is often deployed without sufficient thought as to how it may be abused, alone or in combination with other deployed technologies. There is great incentive for 'the bad guys' to develop attacks, and they do, often with great creativity and speed."

facebook
Facebook helps you connect and share with the people in your life.

Because Web 2.0 applications are particularly vulnerable to exploitation, industry and security experts recommend proactive countermeasures and multi-layered security solutions that include:

- **Application control:** Granular application control, based upon the business and regulatory requirements of the organization, gives organizations the ability to create access policies specific to user identities, and to reduce risks for some employees without restricting participation for others.
- **Next-generation firewalls:** Many firewalls today don't provide effective protection for Web 2.0 technologies. Organizations should consider next-generation firewalls that provide more sophisticated discovery, control, and visualization of applications, along with predictive threat protection for network infrastructures.
- **Endpoint protection:** The shared and highly participatory nature of Web 2.0 requires that businesses protect their endpoints against multiple threats, including spam, viruses, malicious software, spyware, rootkits, and hacker attacks. Endpoint protection remains a critical piece of information assurance and security in organizations.
- **Data loss protection:** Data exfiltration is a continuing challenge of organizations participating in the Web 2.0 environment. Protecting the integrity and confidentiality of organizational information from theft and inadvertent loss is a key issue today. Data loss protection guards private, sensitive, and confidential information and data from accidental or malicious loss.
- **Encryption:** Important data at rest should be encrypted, as should communication channels, with keying material kept separate from the encrypted material. Compromise or loss of endpoints should not automatically give access to sensitive information.
- **Authentication**: Strong, non-password based authentication should be deployed and used for access to sensitive information and resources. Web2.0 applications usually employ weak authentication, and are targets for a chain of penetration and social engineering attacks that can compromise valuable resources. Requiring appropriate token-based or biometric authentication at key points can help to prevent incidents.
- **Integrity Monitoring and Whitelisting:** Many current attacks against Web2.0-enabled hosts involve the installation or modification of code to enable access, or to install malware. Traditional anti-malware technologies are not sufficient to prevent these threats, so additional methods that use configuration integrity monitoring or application whitelisting should be considered. Solutions that monitor and control patching and upgrades should also be considered.
- **Gateway Anti-malware:** Proactive scanning of code in web pages for malicious intent. By analyzing the code at the web gateway—a gateway located physically in the enterprise or in the cloud as a hosted service, malware can be detected and blocked before it reaches the endpoint or other network assets.

While industry experts recommend both policy and technology solutions, as many as 60 percent of organizations do not budget for Web 2.0-specific security solutions, and some have incurred high, unanticipated losses. Organizations in India and Brazil, which have seen high losses from security incidents, are most likely to budget for Web 2.0-specific security solutions. Three quarters of Indian organizations and more than half of Brazilian organizations do so.

Experts agree that the benefits of using Web 2.0 exceed the risks. "The benefits are there and they're real. There is a strong desire by those who are worried about security to avoid risk. There might be areas where that is a rational way to do it, but you cannot NOT communicate from these platforms today. If you don't, you are at a serious disadvantage no matter what kind of organization you are. You have to strike that balance for your organization," explains Commander Scott McIlnay, Director of Emerging Media Integration for the U.S. Navy.

Even in organizations for which security is a topmost concern — the U.S. Department of Defense, the U.S. Navy and national intelligence agencies — the benefits outweigh the risks, and these organizations have embraced social media at several levels.

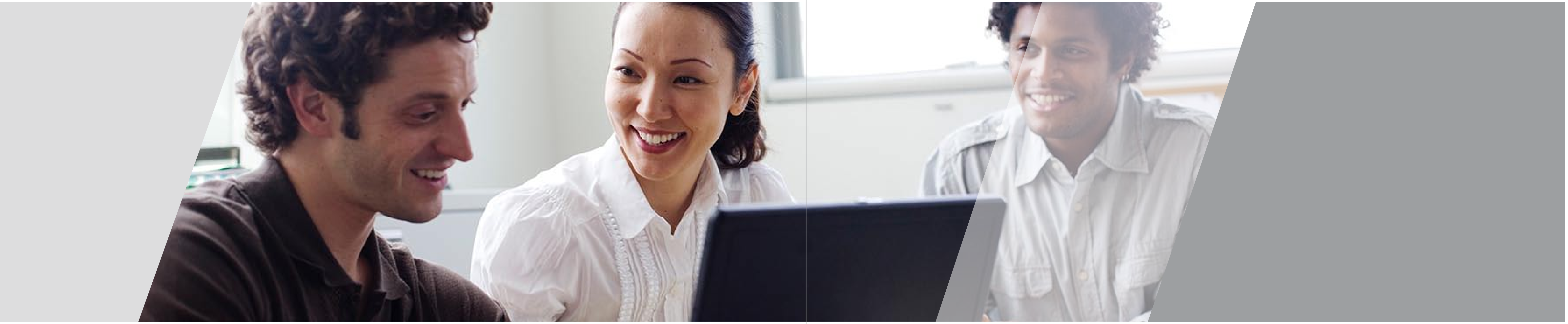
"You can allow employee use of Web 2.0 and absolutely embrace Web 2.0 for your corporate and government goals. But contemplate user behavior and control what goes in and out of your network, and that can be done through both administrative and technical controls," advises McAfee cybercrime strategist, Pamela Warren.

Both IT security experts and industry analysts emphasize the importance of weaving complex security solutions that include policy, technology and education help employees to make good decisions. Echoing cybercrime strategist Warren's comments, industry analyst Dion Hinchcliffe believes writing a social media policy is not enough. Just as employees went through digital literacy training when they first learned how to use email and computerized productivity tools, they now need education about Web 2.0. "Throwing things out to workers and not explaining the implications, not explaining how to use them properly, is, of course, a risk. Education is half of the challenge of ensuring that things we don't want to have happen won't happen."

Eugene Spafford notes the importance of understanding the continuing evolution of the technology, alongside the new norm of heterogeneity and specificity in organizational contexts:

"The key to effective use of new technologies is to apply them in the correct contexts. For instance, applying social media to marketing and sales may result in increased connectivity with clients and business partners. However, applying those same applications in sensitive financial services and proprietary R&D has the potential to lead to significant losses. Organizations that are still in "single network everywhere, same software everywhere" mode will have the most difficulty adjusting to this new paradigm, and to those that follow. Many decision-makers believe that having a homogeneous and uniform environment is less expensive to procure, maintain, and provide employee education. However, there is a longer-term cost in exposure and vulnerability that is now coming into clearer focus; heterogeneity and specificity allow more tailored protections — and uses. Understanding differences in application, technology, policy and users is perhaps the most important factor in success and safety in Web 2.0 environments and beyond."

The power of Web 2.0 technologies as methods of communication, connection, sharing and participation, is seductive, causing some people (and organizations) to adopt tools without considering the potential consequences. This report shows both the widespread interest and some of the widespread concern about Web 2.0 technologies. Both are warranted, as increased sharing not only has the potential to augment business and personal relationships, but also to enable new methods of fraud and attack.



Conclusion

Overall, research suggests that successful organizational use of Web 2.0 is a complex balancing act that requires analyzing challenges and opportunities, mitigating risks, and combining policy, employee education and technology solutions to ensure security.

While the next generation security solutions will be specific to the organization's mission, industry, size, and locale, there are general best practices that we recommend for all organizations that adopt Web 2.0 solutions:

Policy: Web 2.0 environments have created new organizational contexts that challenge traditional norms of professional behavior. Clear social media policies enable employees to make good decisions about their behaviors in these new contexts, and provide examples and guidelines regarding potential threats.

Technology: Web 2.0 applications and technologies require multi-layered security solutions that provide protection against data loss, endpoint security, application control, and infrastructure firewalls.

Education: As new threats and problems emerge it is vital that all users in the organization are made aware of how to protect resources. Social media require a new level of digital literacy, and organizations need to educate employees about the risks and benefits of accessing and participating in these contexts.

Practices: Organizations must acknowledge the 21st century work practices of employees that are global, mobile, and constantly connected. Policies and technology solutions must be device-independent, whether access comes from the desktop, laptop, handheld, or even wearable or embedded devices, and must be location-independent as well. Organizational practices must protect employees and institutional data no matter what they use, and where they are.

Adaptability: Web 2.0 and social media technologies are notable for their rapid change and evolution. Organizations must be alert to new risks, but also adaptable to changes, and open to seeing opportunities for new value that can be embraced for organizational success.

As we enter the second decade of the 21st century, the landscape of communication, information and organizational technologies continues to reflect emerging technological capabilities as well as changing user demands and needs. Web 2.0 is a convenient term used to describe the social technologies of the 21st century that influence the way we interact.

But technological development moves along a continuum, and human creativity and advancements in technology will continue to push the boundaries of how we communicate, share, and interact — as implied by the word 'Web' itself. Cloud computing, immersive reality, geotagging and location-aware computing, ad hoc networking, agent/avatar-based computing, multicore chips, quantum computing, and more are all in research labs or being deployed by early adopters.

These advancements will continue to bring new opportunities and threats, thus requiring agility and continued evolution of resources. Successful organizations will be those that determine where and how to embrace these emergent tools to add new value and agility to their organizations. Success will require careful, on-going efforts to safeguard assets, including infrastructure, data, and employees, along with measured and educated adoption of new cyber technologies.

Appendices

Contributors

Lorraine Kisselburgh, Ph.D., Purdue University

Lorraine G. Kisselburgh is an assistant professor in Communication at Purdue University, and is also affiliated with research institutes at CERIAS and Discovery Park. She began her career as an information analyst and programmer, and directed the development and use of emerging technologies in higher education. She studies organizational communication, the social implications of emerging technologies, privacy, social networks, and collaboration in online groups. She has published in *Communication Yearbook, Management Communication Quarterly, Communication Studies, Journal of Mechanical Design, Journal of Motor Behavior,* and *Acta Psychologica,* and other published books. Dr. Kisselburgh is a member of the Public Policy committee of the ACM, and has served on advisory committees for business intelligence, decision support systems, distance learning, and instructional technology.

Eugene H. Spafford, Ph.D., Purdue University

Eugene H. Spafford is generally acknowledged as one of the senior leaders in information security. Spaf, as he is known to friends and colleagues, has been involved in research, education and the practice of IT security and reliability for over a quarter decade. He is a professor of computer science at Purdue University in the United States and is the founder and executive director of CERIAS. Dr. Spafford is Editor-in-Chief of the journal *Computers & Security*, Chair of the ACM's U.S. Public Policy Council, a Fellow of the ACM, the IEEE, the AAAS, and the (ISC)2, and is a Distinguished Fellow of the ISSA More information is available at http://bio.spaf.us.

Mihaela Vorvoreanu, Ph.D., Purdue University

Dr. Vorvoreanu is an assistant professor in Computer Graphics Technology and Organizational Leadership & Supervision at Purdue University. She studies the socio-cultural impact of new communication technologies. She has published research articles in the *Journal of New Communications Research, Public Relations Review* and the *Journal of Website Promotion* and a book about online public relations: *Web Site Public Relations: How Corporations Build and Maintain Relationships Online*. Dr. Vorvoreanu holds a Ph.D. in Communication from Purdue University.

With assistance from: **Preeti Rao**, graduate student and research assistant, CERIAS, Purdue University.

Additional Contributors

Stowe Boyd, business strategist, Director, 301works.org, President, Microsyntax.org, U.S.

Matthew Gain, Head of Digital Communications Australia, Edelman, Australia

Frank Gruber, Co-Founder, TECH cocktail, U.S.

Jonathan Grudin, Ph.D., Principal Researcher, Adaptive Systems and Interaction, Microsoft, U.S.

Dion Hinchcliffe, Senior Vice President, Dachis Group, U.S.

Shel Holtz, Principal, Holtz Communication + Technology, U.S.

Charlene Li, Founder, Altimeter Group, U.S.

Anthony Maiello, Systems Engineer, GE Energy, U.S.

Commander Scott McIlnay, APR, Director of Emerging Media Integration, Office of Information, U.S. Department of the Navy

Raj Samani, CTO and VP for Europe, Africa, and the Middle East, McAfee, U.K.

Vanda Scartezini, Co-founder and Partner, Polo Consultores Associados & IT Trend, ICANN member, Brazil

Pamela Warren, Cybercrime Strategist, McAfee, U.S.

Steve Widmann, Director of Web Services, Scott & White Healthcare, U.S.

Paull Young, Director of Digital Engagement, charity: water, U.S.

Survey and Interview Methods

The online survey was administered during the period June 14 — July 22, 2010 by international research firm Vanson Bourne. A total of 1055 respondents from 17 countries representing organizations in both public and private sectors participated in the survey.

Recruitment and Sampling

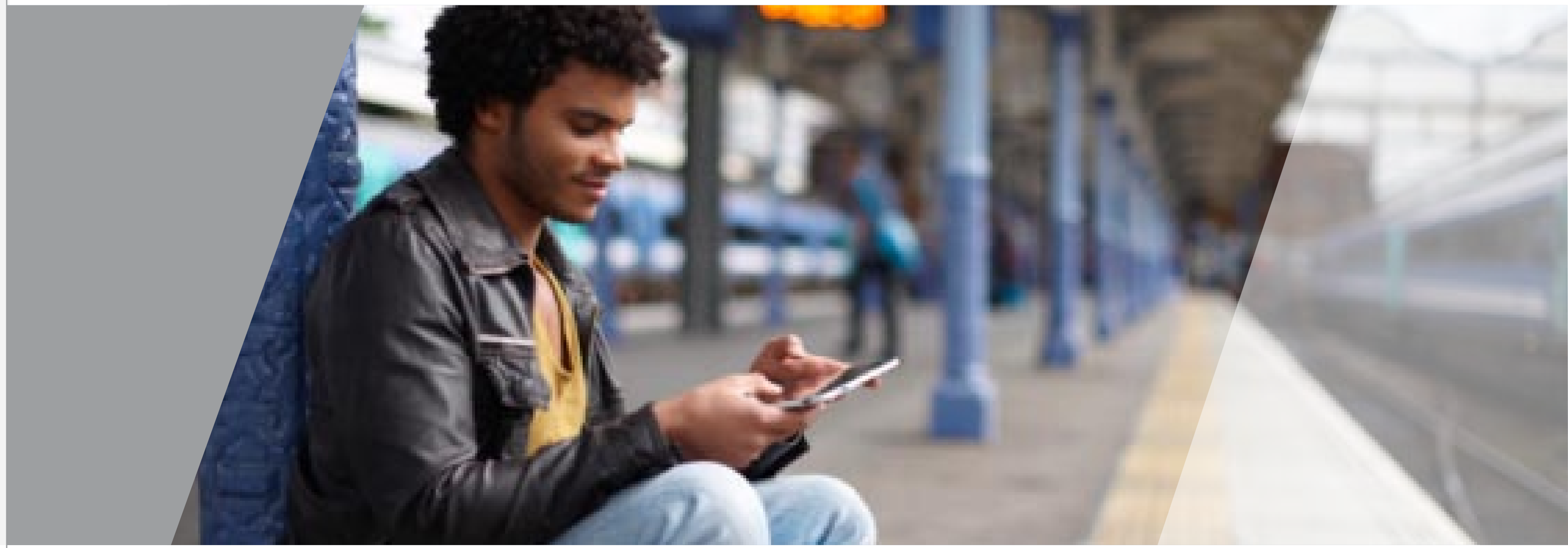
Participants were recruited from multiple sources, including a panel of senior IT decision makers for the UK, an online global B2B sample partner, Global Market Insite and Survey Sampling International. The recruitment sample was pre-screened using criteria established to represent decision-makers, and screened at a second level with initial questions in the survey, to ensure respondents met the criteria for appropriate levels of authority in their organization. Sampling was balanced across organizational size, sector and country. Sixty respondents were sampled from each of 17 countries. Respondents were also sampled from three organizational sizes to achieve a balanced response from small (< 100 PC users), medium (100-1000 PC users) and large (> 1000 PC users) organizations. There was a 19 percent total response rate for the survey, varying from 8 to 42 percent by country.

Interviews

All interviews were conducted in accordance with Purdue University's Institutional Review Board rules for the protection of human subjects. Interviews were conducted with the consent and knowledge of the participants, who gave permission to be identified and quoted in this report. For quotes and case studies available in the public domain, see citation notes for original source.

Respondent Profile

A total of 1055 organizational leaders and decision makers from 17 countries around the globe responded to our survey about current practices and attitudes about Web 2.0 technologies in their organizations. Predominantly CIOs (79 percent) and CEOs (21 percent), the respondents were decision-makers at executive (38 percent), global (15 percent) and national (13 percent) levels in their organizations. Providing a global view, leaders from organizations in 17 countries were surveyed, including respondents from North America (United States, Canada, Mexico), Europe (United Kingdom, Sweden, France, Germany, Benelux, Italy, Spain, Poland), South America (Brazil), Asia (Japan, India, Singapore), Australia and the Middle East (United Arab Emirates). Respondents represented both private sector (63 percent) and public sector (37 percent) organizations, and were drawn equally from small (<100 PC users), medium (<1000 PC users) and large (>1000 PC users) organizations.



About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee secures your digital world.

For more information, visit:
http://www.mcafee.com

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brand may be claimed as the property of others.