

Globale Umfrage über die Risiken sozialer Medien - Überblick

Managementzusammenfassung der Umfrage unter IT- und IT-Sicherheits-Fachleuten
Von Websense gesponsert und vom Ponemon Institute unabhängig durchgeführt

Die Risiken und Chancen sozialer Medien am Arbeitsplatz

Die Nutzung sozialer Medien am Arbeitsplatz nimmt kontinuierlich zu. Unternehmen in aller Welt tauschen sich mit ihren Zielgruppen immer häufiger über Blogs, soziale Netzwerke, Video-on-Demand (VoD), Wikis und andere Verfahren aus. Gleichzeitig nutzen ihre Mitarbeiter soziale Medien tagtäglich – sowohl für geschäftliche als auch für private Zwecke.

Die geschäftlichen Vorteile sozialer Medien müssen vor dem Hintergrund zunehmend gravierender Risiken betrachtet werden: Organisationen müssen sich mit der Möglichkeit von Markenpiraterie auseinandersetzen und sind durch die mangelnde Kontrolle über Inhalte immer größer werdenden Risiken ausgesetzt. Eine der Kernfragen, die Organisationen heute lösen müssen, ist die, wie sie effektiv die besten Optionen zur Verhinderung von Angriffen auf kritische Systeme festlegen können, ohne dabei gleichzeitig eine Integration sozialer Medien in zukünftige geschäftliche Strategien zu verhindern.

An der globalen Umfrage über die Risiken sozialer Medien nahmen 4640 IT- und IT-Sicherheits-Fachleute aus Organisationen in 12 Ländern (USA, Kanada, Großbritannien, Frankreich, Deutschland, Italien, Australien, Singapur, Hongkong, Indien, Brasilien und Mexiko) teil. Diese Zusammenfassung stellt die wesentlichen Erkenntnisse über die Auswirkungen sozialer Medien auf diese Organisationen dar und geht unter anderem auf die Bedeutung sozialer Medien bei der Erreichung geschäftlicher Ziele, auf Richtlinien für die Nutzung sozialer Medien am Arbeitsplatz, sowie auf Sicherheitsrisiken, Sicherheitstechnologien und deren Rolle bei der Minderung von Risiken ein.

Zusammenfassung der wichtigsten Erkenntnisse

Mangelnde Sicherheitskontrollen und Richtlinien

Die Nutzung sozialer Medien am Arbeitsplatz wird zwar für die Erreichung geschäftlicher Ziele als wichtig angesehen, die rapide Verbreitung der Nutzung sozialer Medien scheint zahlreiche Organisationen jedoch auf dem falschen Fuß erwischt zu haben. Es herrscht eine allgemeine Überzeugung vor, dass diese Social Media-Tools ein Risiko für Unternehmen darstellen, und in vielen Fällen fehlen die erforderlichen Sicherheitskontrollen und durchsetzbaren Richtlinien zur Bekämpfung dieser Risiken.

Mitarbeiter als Sicherheitsrisiko

Recherchen zeigen, dass soziale Medien häufiger für private als für geschäftliche Zwecke genutzt werden. Social Networking mit Freunden innerhalb und außerhalb der Organisation wird generell als annehmbar angesehen. Erhebliche Bedenken gibt es jedoch, wenn es darum geht, dass Mitarbeiter Apps oder Widgets von Social Media-Websites herunterladen, unkontrolliert Inhalte posten und ungeprüfte Blog-Einträge erstellen.

Negative Auswirkungen auf Produktivität und Bandbreite

Die Nutzung sozialer Medien hat zu einem Rückgang der Produktivität und zu einer Belastung der IT-Bandbreite geführt. Manche Organisationen haben hierauf reagiert, indem sie ihre Internet-Bandbreite erhöht haben, um eine zunehmende Nutzung sozialer Medien am Arbeitsplatz zu ermöglichen.

Virus- und Malware-Angriffe

Virus- und Malware-Angriffe haben aufgrund der Nutzung sozialer Medien zugenommen. Bei den Technologien, die von den Befragten für die Reduzierung oder Bekämpfung der Bedrohungen durch soziale Medien als besonders wichtig angesehen wurden, handelt es sich um Antivirus-/Anti-Malware-Programme, sichere Web-Gateways (SWG) sowie um Identitäts- und Zugangsmanagement.

Eine globale Perspektive

Bezüglich der Nutzung und der Risiken sozialer Medien am Arbeitsplatz gibt es zwischen den verschiedenen Ländern, in denen die Umfrage durchgeführt wurde, erhebliche Unterschiede im Hinblick auf die jeweiligen Prioritäten, die Wahrnehmung und die entsprechenden Reaktion.

- **Risikowahrnehmung**

In Kanada, Hongkong und Mexiko werden soziale Medien als ernsthafte Bedrohung gesehen, während sie in Frankreich und Italien für weniger riskant gehalten werden. Deutsche Organisationen zeigen sich bezüglich ihrer Fähigkeit zur effektiven Bekämpfung dieser Bedrohungen am zuversichtlichsten.

- **Soziale Medien als wichtiges Geschäftstool**

Organisationen in Großbritannien, Mexiko, Indien, Deutschland und Hongkong messen sozialen Medien eine hohe Bedeutung bei der Erreichung geschäftlicher Ziele bei. In Italien, Australien und Brasilien wird sozialen Medien die geringste Bedeutung zugesprochen.

- **Richtlinien zur Steuerung der Nutzung sozialer Medien**

Deutschland ist das einzige Land, in dem die meisten Befragten angaben, über eine Richtlinie zu verfügen, welche auf eine annehmbare bzw. nicht akzeptable Nutzung sozialer Medien eingeht. In Italien, Singapur und Frankreich sind Organisationen eher der Ansicht, dass ihnen eine entsprechende Richtlinie fehlt.

- **Erhöhte Internet-Bandbreite zur Unterstützung der Nutzung sozialer Medien**

Der größte prozentuale Anteil von Organisationen, die in Bandbreite investiert haben, um die Nutzung sozialer Medien zu ermöglichen, findet sich in Singapur, Großbritannien, Kanada, Australien und Frankreich.

- **Nutzung sozialer Medien für geschäftliche und private Zwecke**

Organisationen in Deutschland verzeichnen die stärkste Nutzung sozialer Medien für geschäftliche Zwecke, während eine private Nutzung am stärksten in den USA, Großbritannien, Frankreich, Italien und Mexiko verbreitet ist. In Deutschland und Indien wird die geringste Anzahl von Minuten verbucht, in denen soziale Medien privat genutzt werden.

- **Virus- und Malware-Angriffe aufgrund der Nutzung sozialer Medien gestiegen**

Befragte in allen Ländern sind der Ansicht, dass ihre Organisationen aufgrund der Nutzung sozialer Medien durch Mitarbeiter am Arbeitsplatz verstärkt Malware-Angriffen ausgesetzt sind. Der geringste Anstieg von Malware-Angriffen aufgrund einer Nutzung sozialer Medien durch Mitarbeiter wurde in Hongkong verzeichnet.

Empfehlungen

IT- und IT-Sicherheits-Experten weltweit erkennen die positiven Auswirkungen, die soziale Medien auf ihre Organisationen haben, wenn es um effektive Vermarktung und Kommunikation geht. Nun stehen sie vor der Herausforderung, sicherzustellen, dass die Nutzung sozialer Medien die Sicherheit ihrer Unternehmensnetzwerke nicht gefährdet.

Risiken erkennen

Um die Risiken, die sich durch soziale Medien am Arbeitsplatz ergeben, verstehen und verwalten zu können, sollten Organisationen eine Risikobeurteilung durchführen, um ein Verständnis dafür zu erlangen, durch welche Praktiken sich möglicherweise Risiken ergeben könnten. Es sollte unmissverständlich an Mitarbeiter kommuniziert werden, wie sich die Nutzung sozialer Medien auf das jeweilige Unternehmen auswirkt. Eine umfassende Richtlinie sollte eingeführt werden, welche auf die jeweiligen Risiken eingeht und Sicherheitsverfahren für alle Mitarbeiter und Sublieferanten, die Social Media-Tools am Arbeitsplatz nutzen, ausführlich darlegt.

Echtzeit-Inhaltssicherheit

Organisationen müssen in der Lage sein, ihre Fähigkeit zur Erkennung und Verhinderung von Angriffen zu verbessern. Das dynamische soziale Web erfordert IT-Sicherheitsmaßnahmen, die über Web-Technologien für eine signaturbasierte Erkennung oder die Durchsetzung vorgegebener Richtlinien hinausgeht. Lösungen wie z.B. Antivirusprogramme oder Firewalls bieten heute keinen angemessenen Schutz vor Bedrohungen mehr. Unternehmen sollten die Vorteile einer Echtzeit-Inhaltssicherheit in Erwägung ziehen, welche Informationen in Echtzeit noch während der Erstellung oder Nutzung analysiert.

Richtlinienkontrollen zur Steigerung der Produktivität

Zu den sozialen Medien zählen unter anderem auch Video-on-Demand (VoD) und Live-Streaming-Ereignisse, die starke Auswirkungen auf die verfügbare Bandbreite haben. Produktivitäts- und Bandbreitenprobleme können beispielsweise durch Zeitkontingente, Bandbreitenmanagement oder Coaching in den Griff bekommen werden. Wenn derartige Kontrollen vorliegen, kann Mitarbeitern die Freiheit des sozialen Webs geboten werden – die Richtlinien stellen sicher, dass die Produktivität gewahrt wird und die Ressourcennutzung dem gewünschten Niveau entspricht.

Soziale Medien: die kommende Herausforderung

Soziale Netzwerke werden für die Erreichung der geschäftlichen Ziele von Organisationen als unersetzlich angesehen, nicht zuletzt zur Steigerung des Bekanntheitsgrads einer Marke, zur Stärkung des Images, zur Sammlung von Daten über Zielgruppen und somit zur Verbesserung von Produkten und Dienstleistungen.

Je mehr sich die Technologien für soziale Medien und die Sicherheit für diese Tools weiterentwickeln, desto mehr werden sich Organisationen, die einen strategischen Ansatz für die Erkennung, die Verwaltung und die Kontrolle der damit verbundenen Risiken gewählt haben, in einer optimalen Position finden, um sich die unbestreitbaren Vorteile dieser Technologie zunutze zu machen.



Global Survey on Social Media Risks

Survey of IT & IT Security Practitioners

Sponsored by Websense

Independently conducted by Ponemon Institute^{LLC}

Publication Date: September 2011

Global Survey on Social Media Risks

Survey of IT & IT Security Practitioners

Ponemon Institute, September 2011

Part 1: Introduction

The use of social media in the workplace is growing at a rapid pace. Savvy businesses are using blogs, social networks, video on demand (VoD), wikis and other vehicles to quickly share information with their target audiences. The result can be greater brand awareness and an enhanced image in the marketplace. Social media can also play an important role in gathering intelligence directly from an organization's target audience to help improve products, services and other areas of their business. As social media technology and the security for these tools continue to evolve, we imagine organizations will realize even more benefits.

Along with these benefits have come risks. ISACA has identified the following as the top five risks of social media: viruses/malware, brand hijacking, lack of control over content, unrealistic customer expectations of "Internet-speed" service and non-compliance with record management regulations.¹

Ponemon Institute is pleased to present the findings of our study, *Global Survey on Social Media Risks*. Sponsored by Websense, we believe this is the first study conducted to determine what IT and IT security practitioners throughout the world think about security risks associated with employees' use of social media tools.

As the study reveals, social media is now considered important for an organization's ability to achieve its business objectives. Our purpose is to understand the magnitude of the risk and what actions might be taken to prevent attacks on systems and still allow businesses to integrate the use of social media into their business strategies.

The study surveyed 4,640 IT and IT security practitioners in the United States, Canada, United Kingdom, France, Germany, Italy, Australia, Singapore, Hong Kong, India, Brazil and Mexico with an average of 10 years experience in the field. Fifty-four percent hold positions of supervisor or above and 42 percent are employed by organizations with a headcount of more than 5,000.

In this study we asked IT and IT security practitioners in these countries about the following issues:

- The importance of social media in meeting business goals today.
- The existence of enforceable policies governing the use of social media tools in the workplace.
- The security risks created by employee usage of social media tools.
- The use of enabling security technologies to reduce or mitigate social media risks.

We believe the following are the most salient findings from this study:

- Most respondents agree that the use of social media in the workplace is important to achieving business objectives. However, they also believe these tools put their organizations at risk and they do not have the necessary security controls and enforceable policies to address the risk.
- Organizations are most concerned with employees downloading apps or widgets from social media sites, posting uncensored content and uncensored blog entries.

¹ Top Five Social Media Risks for Business: ISACA White Paper, June 7, 2010

- Employees are using social media tools more often for non-business purposes than business purposes.
- Malware infections are increasing as a result of social media use. Technologies considered by respondents to be most important to reducing or mitigating social media threats are anti-virus/anti-malware, secure web gateway (SWG) and identity and access management.
- Organizations are increasing their Internet bandwidth to accommodate the increased use of social media in the workplace.

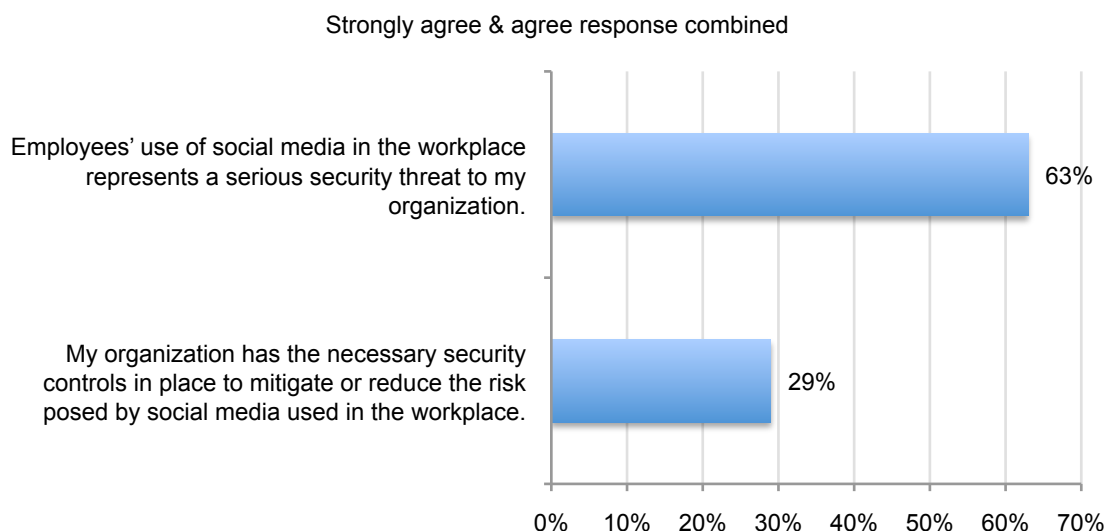
Part 2. Analysis of key findings

In this section, we examine the impact social media is having on organizations and how organizations are responding to the risks we described previously.

The rapid proliferation in the use of social media may have caught many organizations off guard. As shown in Bar Chart 1, most respondents (63 percent) agree that employees' use of social media puts their organizations' security at risk. In contrast, only 29 percent say they have the necessary security controls in place to mitigate or reduce the risk posed by social media used in the workforce.

According to Websense, potential threats exist because social circles provide a trusted attack position for cybercrime between friends when account credentials are compromised. Lures and dynamic web links can quickly infect friends and then infect their social circles. The other aspect of social media is providing cybercrime user profile information for spear-phishing and customized lures individuals are more likely to accept.

Bar Chart 1: Two attributions about the use of social media and the threat it poses in the workplace.

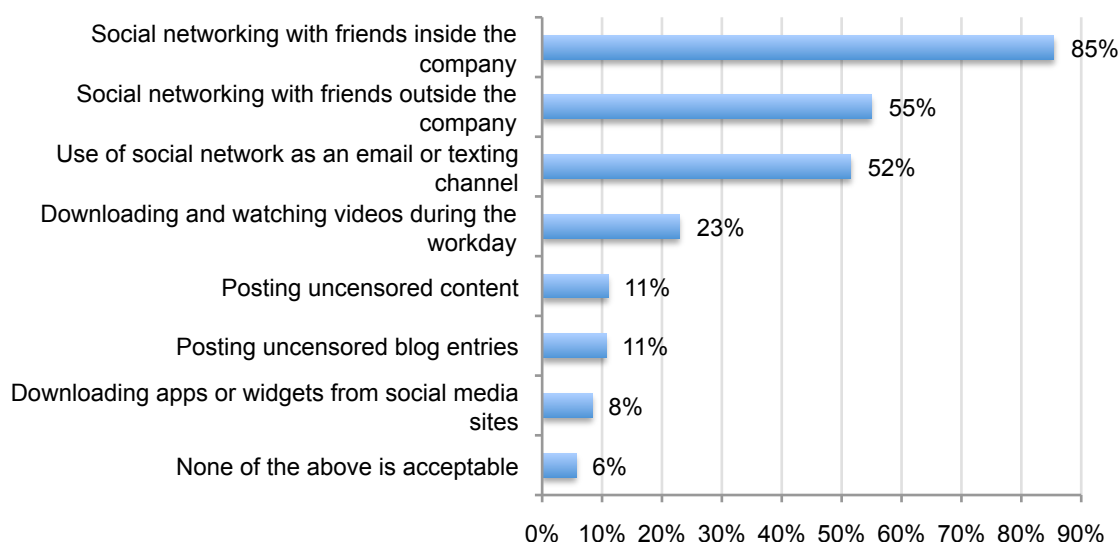


If there is a policy to address the acceptable use of social media in the workplace, 65 percent say their organizations do not enforce it or they are unsure. The top three reasons for not enforcing these policies are lack of governance and oversight (44 percent), other security issues are a priority (43 percent) and insufficient resources to monitor compliance with the policy (41 percent).

Organizations say the use of social networking with friends inside and outside the organization is acceptable. Based on this response, we believe organizations consider social media a positive tool for encouraging collaboration and building internal relationships. However, the blending of the social and work environment does create risk because devices the organization does not own are on the network and the exchange of content among employees cannot be controlled.

Bar Chart 2 reveals that 85 percent of respondents and 55 percent say it is acceptable to use social networking inside the company to communicate with friends. However, a much smaller percentage (11 percent) of respondents say posting uncensored content or blog entries on the network is acceptable and 8 percent say downloading apps or widgets from social media sites is not acceptable.

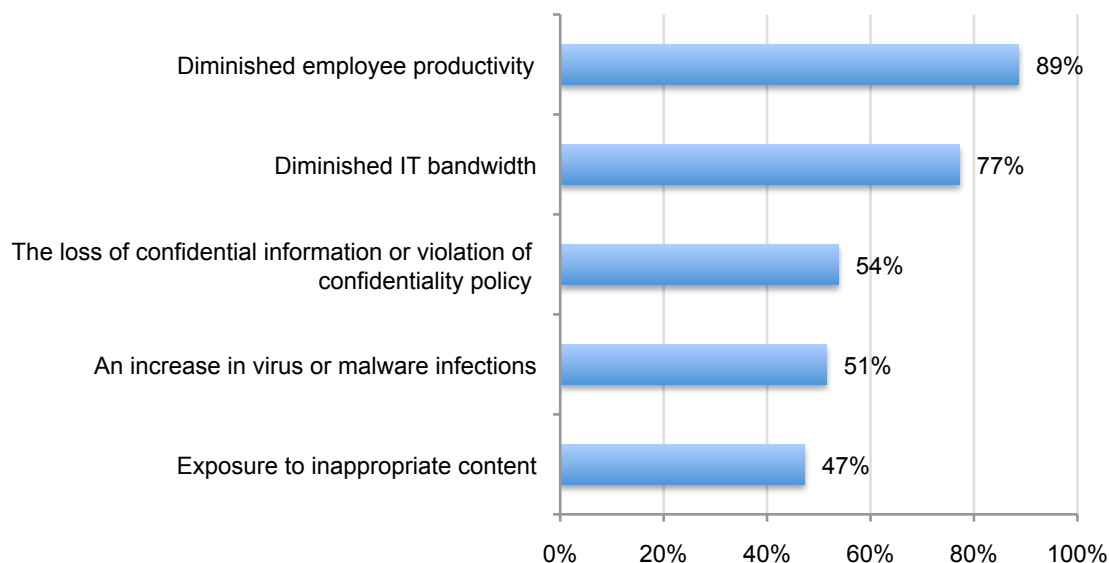
Bar Chart 2: What is considered the acceptable use of social media in the workplace



Organizations believe productivity has declined and IT bandwidth has been diminished as a result of social media usage. The top two negative consequences of an increase in social media in the workplace are shown in Bar Chart 3. These are: diminished productivity (89 percent) and diminished IT bandwidth (77 percent). Less than half (47 percent) believes exposure to inappropriate content is a negative consequence. Fifty-nine percent of organizations in the study increased their Internet bandwidth (pipe) to accommodate employees' use of social media during the past 12 months.

Bar Chart 3: Consequences of social media usage in the workplace

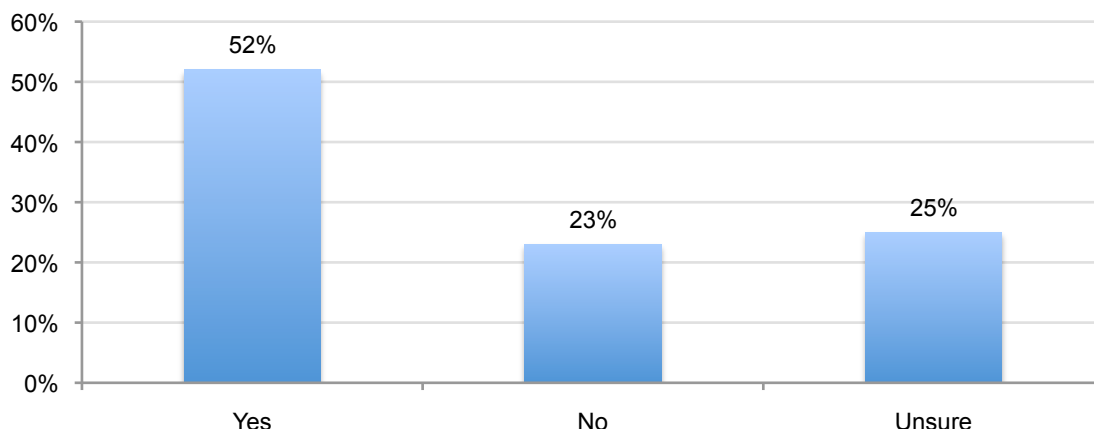
Each bar represents the percent of respondents who said the issue has already happened or is very likely to occur.



A reason for the need to increase bandwidth, according to Websense, is that social media includes video-on-demand (VoD) and live streaming events that will drive up bandwidth consumption. These viral videos and images gaining quick popularity from social circles between friends also make excellent lures for web threats. The web also has been a productivity concern for management since inception. However, with quotas and bandwidth controls employees can have access within reasonable boundaries keeping productivity at desirable levels.

Virus and malware attacks have increased because of social media usage. Bar Chart 4 shows that 52 percent of organizations experienced an increase in malware attacks as a result of employees' use of social media and 27 percent say these attacks increased more than 51 percent.

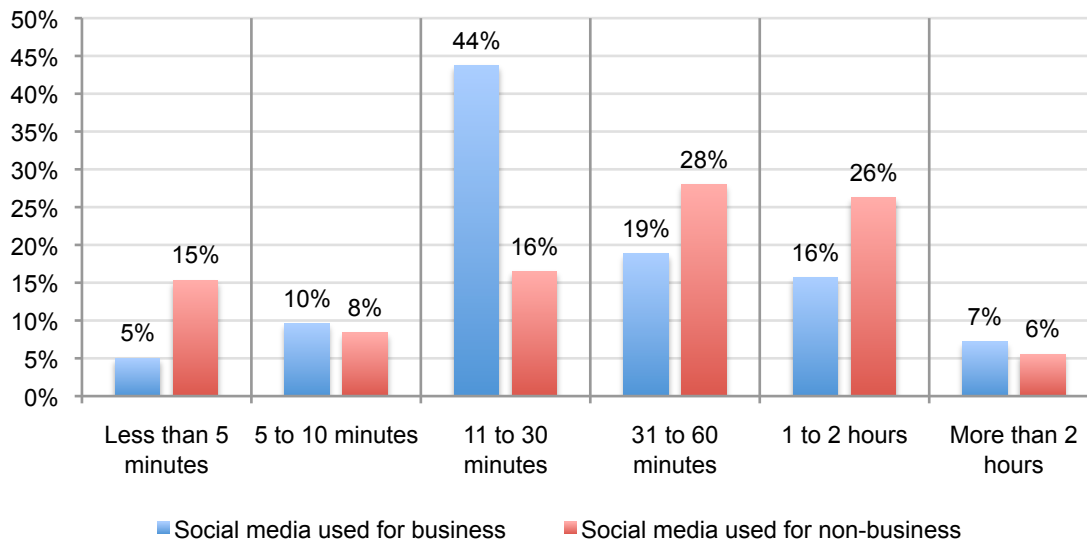
Bar Chart 4: Did your organization experience any increase in virus and malware attacks as a result of employees' use of social media in the workplace?



Social media is more often used for personal reasons. Employees are using social media for both business and non-business purposes. However, they are using it more often for personal reasons. About half (47 percent) use social media more than one-third of the time (37 percent) for business however 63 percent use social media for non-business purposes more than one-third of the time (37 percent).

Time spent on social media for business and non-business purposes also varies, as shown in Bar Chart 5. Fifty-nine percent use social media no more than 30 minutes per day for business reasons. However, 60 percent of employees are estimated to use social media for personal reasons at least 30 minutes per day.

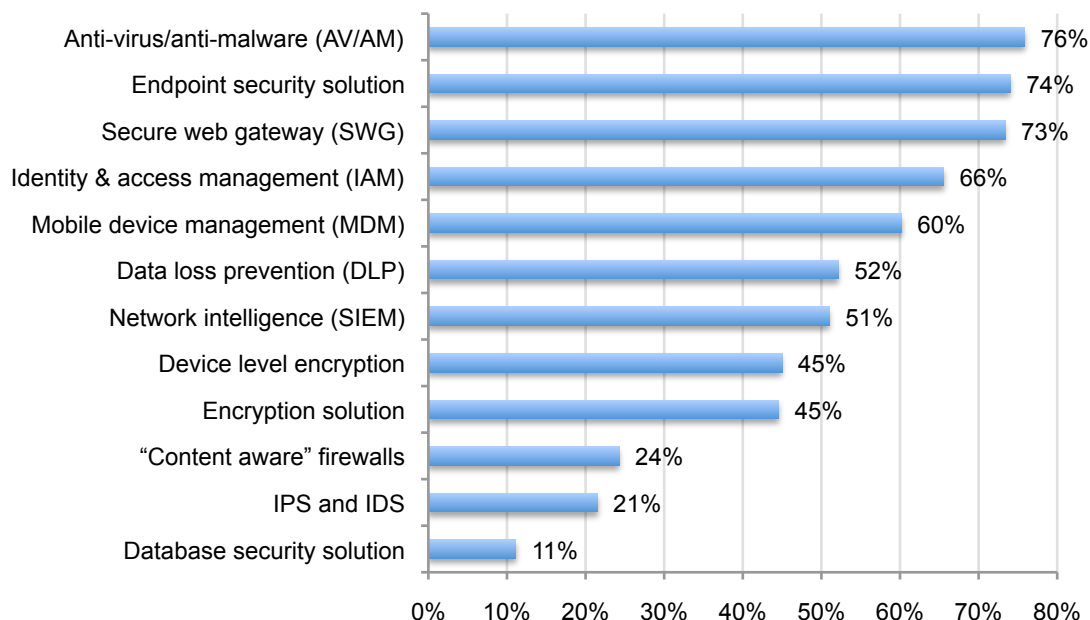
Bar Chart 5: Approximate time spent by employees on social media during the workday



To mitigate the risks created by social media certain technologies are preferred.

Bar Chart 6 shows the technologies that respondents consider most important to reducing or mitigating social media threats are anti-virus/anti-malware, endpoint security solutions and secure web gateway.

Bar Chart 6: Enabling security technologies that are viewed as essential or very important for reducing the risks caused by social media in the workplace



According to Websense, the dynamic social web requires an IT security defense that goes beyond signature and fixed-policy web technologies (like anti-virus and firewalls). New technologies such as social media, cloud services and mobility require real-time content security, which analyzes information in real-time as it is created and consumed. Further, Websense says that traditional defenses such as anti-virus do not provide appropriate threat protection.

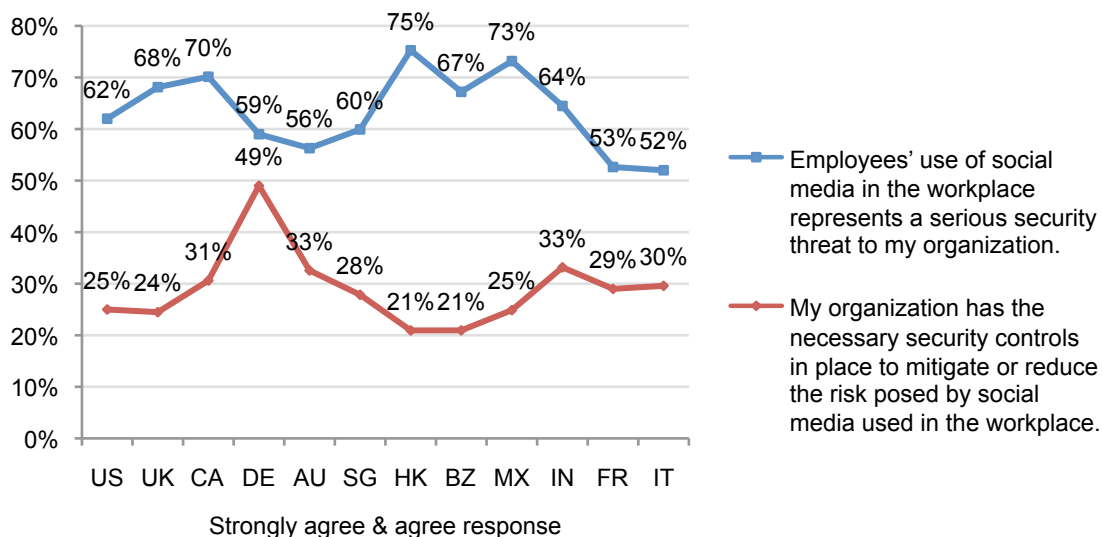
Part 3. Most significant country differences

In this section, we provide an analysis of the different perceptions among IT and IT security practitioners in 12 countries concerning the use of social media in their organizations.²

Perception of risk. As shown in Line Graph 1, countries with organizations that are most likely to see social media as a serious threat to their organization: Canada, Hong Kong and Mexico. Countries least likely to see social media as a threat are France and Italy. The country with organizations that have the most confidence in their ability to address the threat is Germany.

Line Graph 1: Two attributions on social media and the risk it poses in the workplace

Results shown for 12 separate country samples

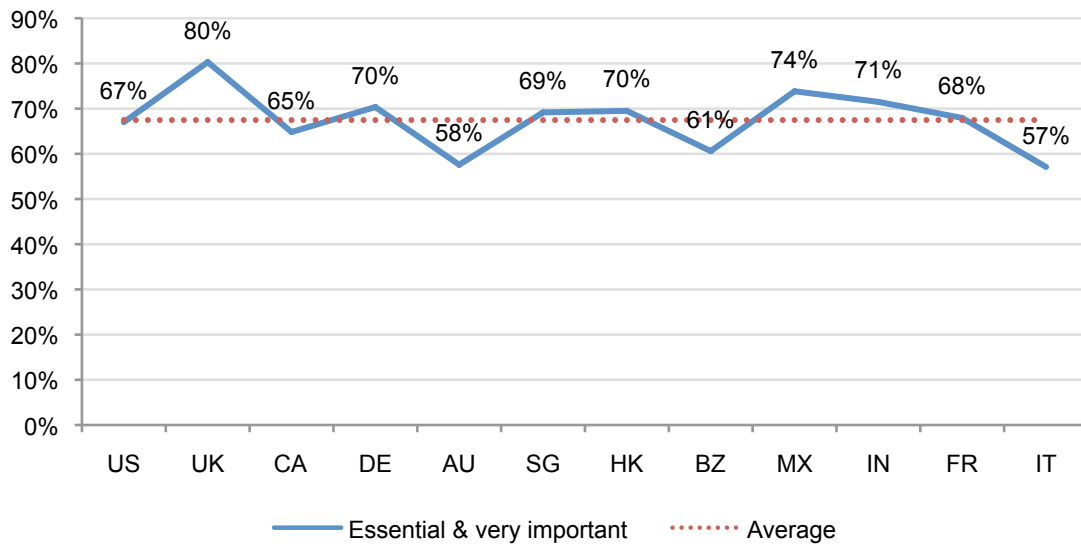


² The horizontal axis to each line graph represents the individual country sample. See Table 1 (Methods section) for country legend used in this section.

Social media as an important tool for business. The countries with organizations that are most likely to see social media as important to meeting business objectives are: U.K., Mexico, India, Germany and Hong Kong (Line Graph 2). The countries with organizations that are less likely to see the importance of social media are: Italy, Australia and Brazil.

Line Graph 2: How important is social media in terms of meeting business objectives in your organization?

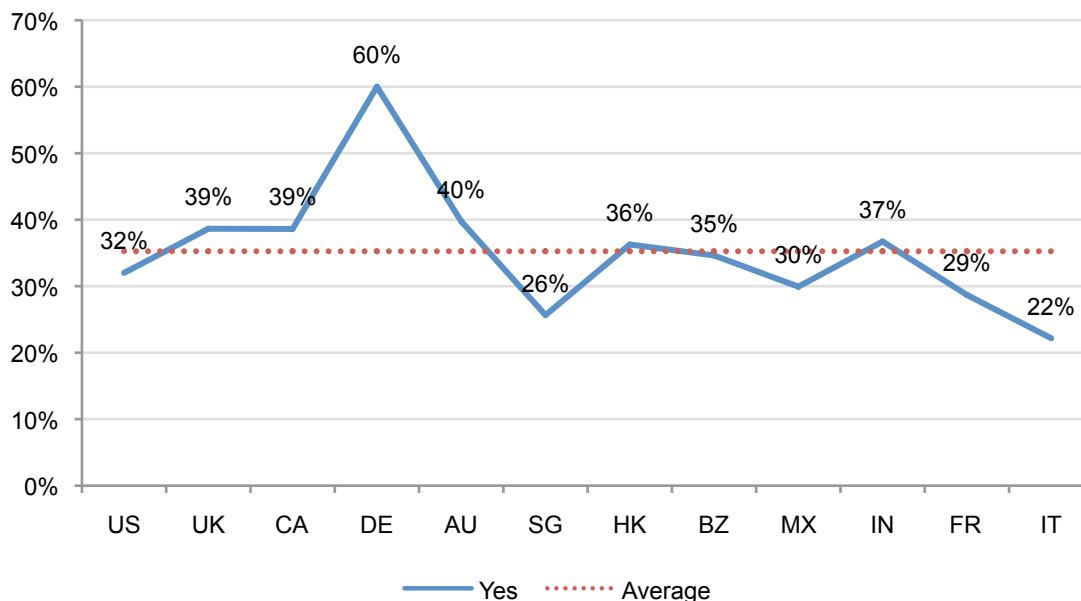
Results shown for 12 separate country samples



Policies to address social media usage. Line Graph 3 reveals that Germany is the only country with the most organizations that believe they have a policy that addresses the acceptable or unacceptable use of social media. Countries with organizations that are more likely to believe they are lacking such a policy are Italy, Singapore, and France.

Line Graph 3: Does your organization have a policy that addresses the acceptable use of social media by employees in the workplace?

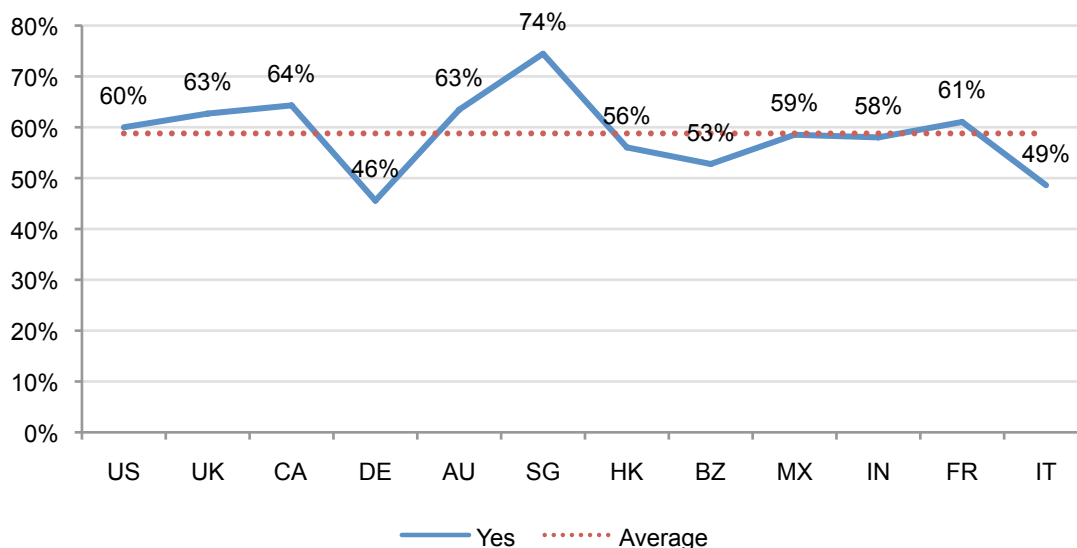
Results shown for 12 separate country samples



Increased Internet bandwidth to support social media usage. Singapore, United Kingdom, Canada, Australia and France are countries where the greatest percentage of organizations invested in bandwidth to enable the use of social media. (see Line Graph 4).

Line Graph 4: Did your organization increase its Internet bandwidth (pipe) to accommodate employees' use of social media during the past 12 months?

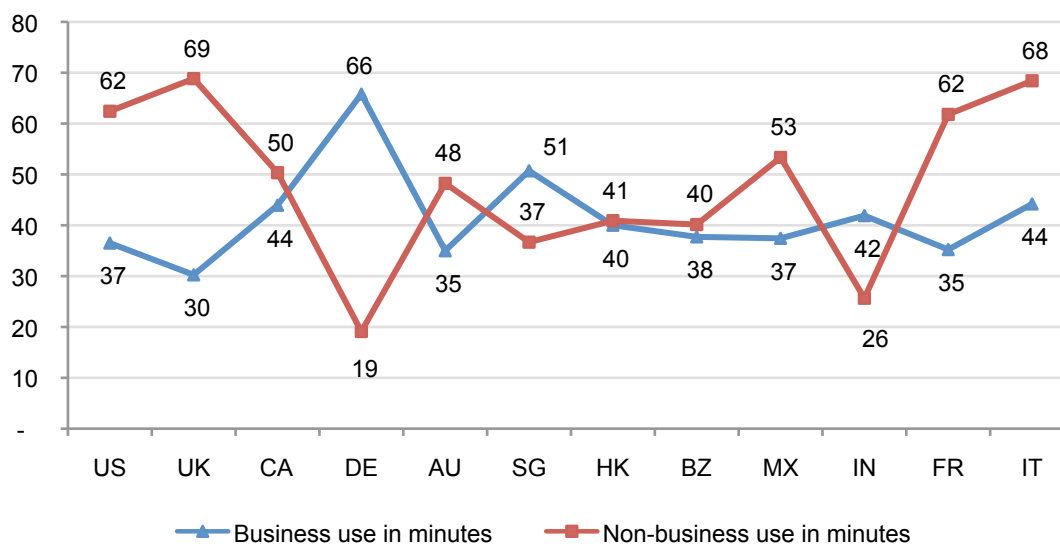
Results shown for 12 separate country samples



Use of social media for business and non-business purposes. According to Line Graph 5, organizations in Germany are more likely to have the highest use of social media for business purposes. Countries where there is the highest use of social media for non-business reasons are: U.S., U.K., France, Italy, and Mexico. The countries with the least amount of minutes used for personal reasons are Germany and India.

Line Graph 5: Business and non-business use of social media expressed in minutes used per day

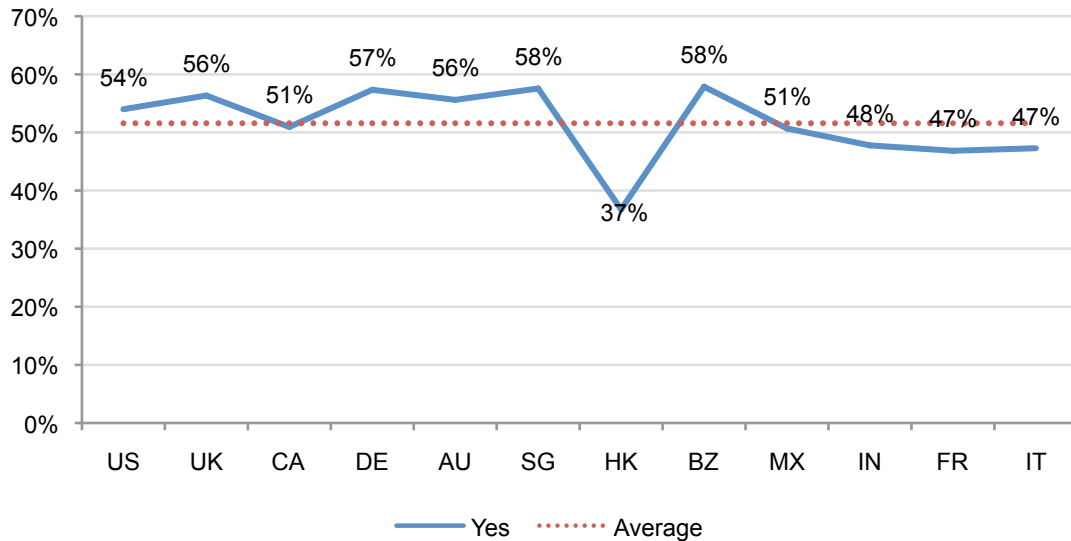
Results shown for 12 separate country samples



Virus and malware attacks as a result of social media usage. As shown in Line Graph 6, respondents in Hong Kong report the lowest level of increase in malware attacks as a result of employees' use of social media. Singapore, Brazil and Germany report the highest increase in such attacks. Overall results clearly show that respondents in all countries believe their organizations suffered from an increase in malware activities as a result of social media used by employees in the workplace.

Line Graph 6: Did your organization experience any increase in virus and malware attacks as a result of employees' use of social media?

Results shown for 12 separate country samples



Part 4: Methods

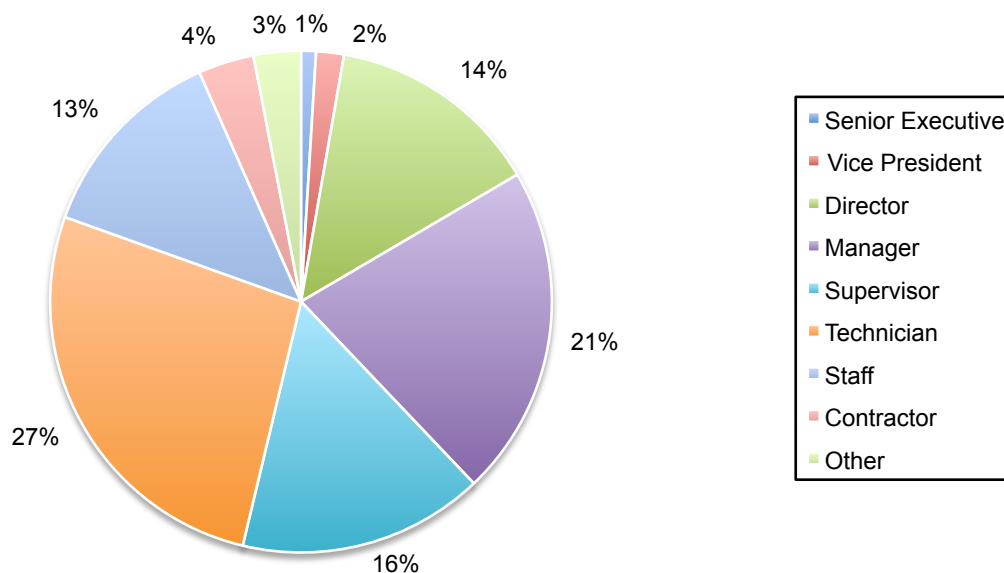
Table 4 reports the sample response for 12 separate country samples. The sample response for this study conducted over a 30-day period ending in July 2011. Our consolidated sampling frame of practitioners in 12 countries consisted of 116,491 individuals who have bona fide credentials in the IT or IT security fields. From this sampling frame, we captured 5,131 returns of which 491 were rejected for reliability issues. Our final consolidated sample before screening was 4,640, thus resulting in a 4.0% response rate.

Table 1: Sample response for 12 countries						
Country	Legend	Sample frame	Returns	Rejections	Final sample	Response rate
United States	US	15,775	655	54	601	3.8%
United Kingdom	UK	9,885	419	32	387	3.9%
Canada	CA	8,701	451	30	421	4.8%
Germany	DE	11,063	560	25	535	4.8%
Australia	AU	6,503	329	29	300	4.6%
Singapore	SG	5,003	277	18	259	5.2%
Hong Kong	HK	4,993	256	35	221	4.4%
Brazil	BZ	11,090	504	76	428	3.9%
Mexico	MX	12,509	398	52	346	2.8%
India	IN	13,010	560	49	511	3.9%
France	FR	9,005	367	40	327	3.6%
Italy	IT	8,954	355	51	304	3.4%
Total		116,491	5,131	491	4,640	4.0%

Pie Chart 1 summarizes the approximate position levels of respondents in our study. As can be seen, the majority (54 percent) of respondents are at or above the supervisory level. The respondents' average experience in IT or IT security is 10.35 years.

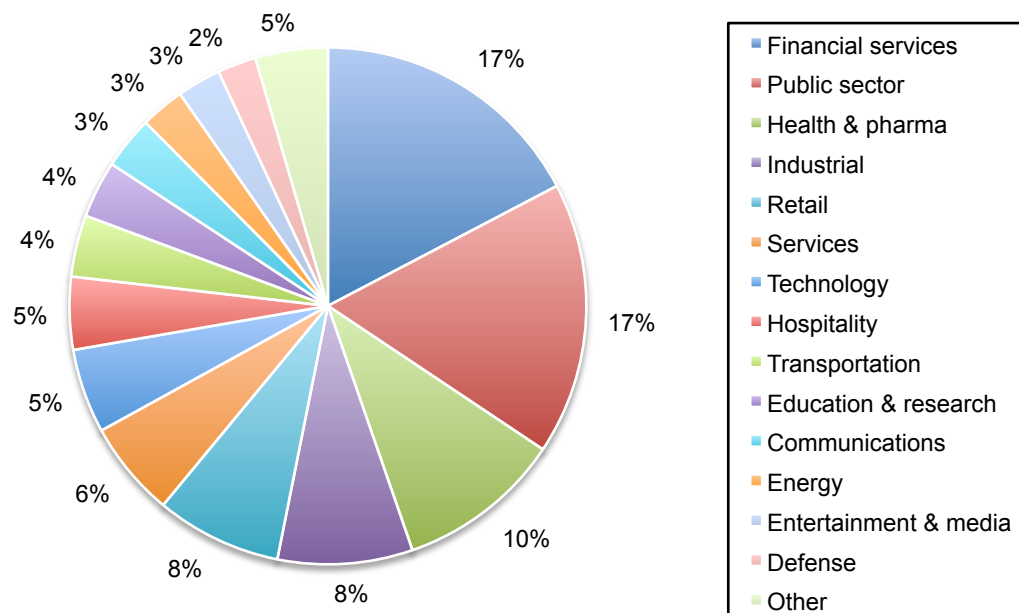
Pie Chart 1: Distribution of respondents according to position level

Consolidated for 12 separate country samples



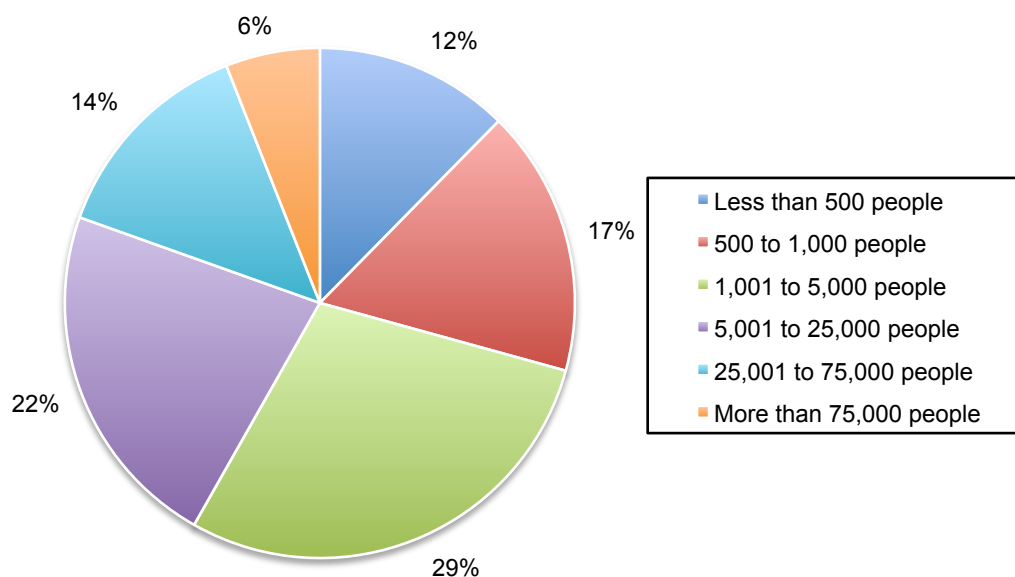
Pie Chart 2 reports the respondents' organizations primary industry segments. As shown, 17 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 17 percent are located in public sector organizations, including central and local government.

Pie Chart 2: Distribution of respondents according to primary industry classification
Consolidated for 12 separate country samples



According to Pie Chart 3, the majority of respondents (71 percent) are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Pie Chart 3: Distribution of respondents according to organizational headcount
Consolidated for 12 separate country samples



Part 5: Recommendations & Caveats

In every part of the globe, IT and IT security practitioners recognize the positive impact social media is having on their organizations' ability to market and communicate effectively. The challenge they face is how to ensure the use of social media vehicles does not jeopardize the security of their organizations' networks. We believe that specific steps can be taken to reduce the risk without hindering the opportunities social media offers. To achieve the right balance between enabling the use of social media and protecting the organization's network from attacks, we have the following recommendations:

- Understand the risk social media tools create in the workplace. Conduct a risk assessment to understand what practices may be putting the organization at risk.
- Educate employees about how their social media usage could impact the company. For example, how posting something inappropriate could breach company security and hurt its reputation.
- Create a comprehensive policy (including detailed guidelines) for all employees and contractors who use social media tools in the workplace. The policy should address the risks and the security procedures that should be followed.
- Improve the ability through expertise and enabling technologies to detect and prevent attacks.
- Consider the use of time quotas, bandwidth management and coaching to allow employees the freedom of the social web with policy controls to keep productivity and resource utilization in check.

Limitations

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in 12 countries, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners who deal with network or security issues. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

Appendix: Audited Findings

The following tables report the percentage frequencies for all survey questions relating to social media in the workplace (Part 1). The consolidated values for 12 separate country samples are reported. See Table 1 for additional details. Please note that Part 2 of the survey instrument is not reported here. These additional survey questions pertain to the use of mobile devices in the workplace and will be presented in a future report. All survey responses were gathered in July 2011.

Country samples	Consolidated
Sample frame	116,491
Returned surveys	5,131
Rejected surveys	491
Final sample	4,640
Response rate	4.0%

Part 1. Social media

Attributions: Five-point scale from strongly agree to strongly disagree. Reported is strongly agree and agree responses combined.	Consolidated
Q1a. Employees' use of social media in the workplace represents a serious security threat to my organization.	63%
Q1b. My organization has the necessary security controls in place to mitigate or reduce the risk posed by social media used in the workplace.	29%

Q2. How important is the use of social media in terms of meeting business objectives in your organization today? Scale is from essential to irrelevant. Reported is essential and very important combined.	67%
--	-----

Q3a. Does your organization have a policy that addresses the acceptable or unacceptable use of social media by employees?	Consolidated
Yes	35%
No	41%
Unsure	24%
Total	100%

Q3b. If yes, is this policy enforced?	Consolidated
Yes	35%
No	43%
Unsure	22%
Total	100%

Q3c. If you answered no in Q3b, then why isn't the policy enforced? Please select only two choices.	Consolidated
Insufficient resources to monitor compliance with the policy	41%
Other security issues are a priority	43%
Lack of management concern	30%
Lack of technology solutions	32%
Lack of governance and oversight	44%
Other (please specify)	4%

Q4. Which single statement best describes the acceptable use of social media within your organization?	Consolidated
We allow all employees to use social media to increase their productivity or as a job perk	38%
We allow only specified employees to use social media to increase their productivity or as a job perk	26%
We do not allow employees to use social media in the workplace	36%

Total	100%
-------	------

Q5. If your organization allows employees to use social media in the workplace, what is considered an acceptable use?	Consolidated
Social networking with friends inside the company	85%
Social networking with friends outside the company	55%
Downloading and watching videos during the workday	23%
Downloading apps or widgets from social media sites	8%
Use of social network as an email or texting channel	52%
Posting uncensored content	11%
Posting uncensored blog entries	11%
None of the above is acceptable	6%
Other (please specify)	1%
Total	251%

Q6. Please rate the likelihood of each one of the following issues occurring due to an increase in the use of social media in the workplace. Please use the five-point scale provided below each item from already happened to never. Reported is already happened and very likely to happen combined responses.	Consolidated
Q6a. Diminished IT bandwidth	77%
Q6b. Diminished employee productivity	89%
Q6c. The loss of confidential information or violation of confidentiality policy	54%
Q6d. An increase in malware infections	51%
Q6e. Exposure to inappropriate content (e.g., nudity, violence, etc.)	47%

Q7a. Did your organization increase its Internet bandwidth (pipe) to accommodate employees' use social media during the past 12 months?	Consolidated
Yes	59%
No	26%
Unsure	15%
Total	100%

Q7b. Approximately, how large was this increase in your organization's Internet bandwidth (pipe)? Your best guess is welcome.	Consolidated
Less than 1 MB	20%
1 to 3 MB	40%
4 to 5 MB	31%
More than 5 MB	9%
Total	100%

Q8a. Did your organization experience any increase in virus or malware attacks as a result of employees' use of social media?	Consolidated
Yes	52%
No	23%
Unsure	25%
Total	100%

Q8b. If yes, approximately (in percentage terms) how much did viruses and malware infections increase as a result of employees' use of social media? Your best guess is welcome.	Consolidated
Less than 10%	11%
10 to 25%	18%
26 to 50%	31%
51 to 100%	14%
101 to 200%	10%
More than 200%	3%
Don't know	11%

Total	100%
-------	------

Q9. Approximately, what percentage of employees in your organization use social media for business reasons during the workday?	Consolidated
None	28%
1 to 10%	5%
11 to 25%	6%
36 to 50%	16%
51 to 75%	18%
76 to 100%	13%
Don't know	14%
Total	100%

Q10. Approximately, what percentage of employees in your organization use social media for non-business (personal) reasons during the workday?	Consolidated
None	11%
1 to 10%	3%
11 to 25%	8%
36 to 50%	12%
51 to 75%	15%
76 to 100%	36%
Don't know	16%
Total	100%

Q11a. Social media used for business purposes during the workday:	Consolidated
Less than 5 minutes	5%
5 to 10 minutes	10%
11 to 30 minutes	44%
31 to 60 minutes	19%
1 to 2 hours	16%
More than 2 hours	7%
Total	100%

Q11b. Social media used for non-business purposes during the workday:	Consolidated
Less than 5 minutes	15%
5 to 10 minutes	8%
11 to 30 minutes	16%
31 to 60 minutes	28%
1 to 2 hours	26%
More than 2 hours	6%
Total	100%

Q12. In your opinion, how important is each one of the following enabling security technologies at reducing or mitigating social media security threats? Please indicate your opinion using the following scale: From essential to irrelevant. Reported are essential and very important combined responses.	Consolidated
Mobile device management (MDM)	60%
Data loss prevention (DLP)	52%
Anti-virus/anti-malware (AV/AM)	76%
Intrusion prevention (IPS) & intrusion detection (IDS)	21%
"Content aware" firewalls	24%
Identity & access management (IAM)	66%
Endpoint security solution	74%
Database security solution	11%
Device level encryption	45%
Network intelligence (SIEM)	51%
Encryption solution	45%
Secure web gateway (SWG)	73%
Other (please specify)	6%
Total	605%

Part 3. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	1%
Vice President	2%
Director	14%
Manager	21%
Supervisor	16%
Technician	27%
Staff	13%
Contractor	4%
Other	3%
Total	100%

D2. Total years of relevant experience	Consolidated
Total years of IT or security experience	10.35
Total years in current position	4.70

D3. Check the Primary Person you or your IT security leader reports to within the organization.	Consolidated
CEO/Executive Committee	1%
Chief Financial Officer	3%
General Counsel	1%
Chief Information Officer	62%
Compliance Officer	11%
Human Resources VP	1%
CISO/CSO	14%
Chief Risk Officer	3%
Other	6%
Total	100%

D4. What industry best describes your organization's industry focus?	Consolidated
Communications	3%
Defense	2%
Education & research	4%
Energy	3%
Entertainment & media	3%
Financial services	17%
Health & pharmaceuticals	10%
Hospitality	5%
Industrial	8%
Public sector	17%
Retail	8%
Services	6%
Technology	5%
Transportation	4%
Other	5%
Total	100%

D5. Where are your employees located? (Check all that apply):	Consolidated
United States	87%
Canada	63%
Europe	67%
Middle East & Africa	38%
Asia-Pacific	70%
Latin America (including Mexico)	68%

D6. What is the worldwide headcount of your organization?	Consolidated
Less than 500 people	12%
500 to 1,000 people	17%
1,001 to 5,000 people	29%
5,001 to 25,000 people	22%
25,001 to 75,000 people	14%
More than 75,000 people	6%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.