

ENCUESTA GLOBAL SOBRE LOS RIESGOS DE LOS MEDIOS SOCIALES – DESCRIPCIÓN GENERAL

Resumen de la gerencia sobre la encuesta de profesionales de TI y de seguridad de TI
Patrocinada por Websense y realizada por el Instituto Ponemon de manera independiente

Los riesgos y las recompensas de los medios sociales en el lugar de trabajo

El uso de los medios sociales en el lugar de trabajo está aumentando con rapidez. Las empresas de todo el mundo comparten cada vez más información con su público a través de blogs, redes sociales, video a pedido (VoD), wikis y otros medios. Al mismo tiempo, sus empleados utilizan los medios sociales a diario tanto con fines empresariales como no empresariales.

Las ventajas comerciales de los medios sociales deben considerarse en el contexto de riesgos cada vez más graves: los virus y el malware son cada vez más frecuentes, y las organizaciones se enfrentan con la posibilidad del robo de la marca y están cada vez más amenazadas por la falta de control del contenido. Se ha vuelto imperioso determinar el mejor modo de actuar para prevenir ataques en los sistemas críticos y, al mismo tiempo, permitir la integración de los medios sociales en las estrategias empresariales futuras.

En la Encuesta global sobre los riesgos de los medios sociales participaron 4640 profesionales de TI y de seguridad de TI de organizaciones de 12 países (Estados Unidos, Canadá, el Reino Unido, Francia, Alemania, Italia, Australia, Singapur, Hong Kong, India, Brasil y México). Este resumen describe los resultados clave del impacto de los medios sociales en estas organizaciones, e incluye la importancia de los medios sociales para alcanzar los objetivos empresariales, las políticas que rigen el uso de los medios sociales en el lugar de trabajo, los riesgos de seguridad, y las tecnologías de seguridad y el papel que desempeñan en la mitigación de riesgos.

Resumen de resultados clave

Falta de controles y políticas de seguridad

Si bien el uso de los medios sociales en el lugar de trabajo se considera muy importante para alcanzar los objetivos empresariales, la rápida proliferación del uso de los medios sociales parece haber tomado desprevenidas a muchas organizaciones. En general, se cree que estas herramientas de medios sociales ponen a sus empresas en riesgo y no se dispone de controles de seguridad necesarios y políticas aplicables para hacer frente a los riesgos.

Los empleados como un riesgo de seguridad

La investigación muestra que los medios sociales se utilizan con más frecuencia por motivos personales que por razones comerciales. Los vínculos sociales con amigos dentro y fuera de la organización generalmente se consideran aceptables, si bien se expresaron graves preocupaciones por empleados que descargan aplicaciones o widgets de sitios de medios sociales y publican contenido no censurado y entradas en blogs no censuradas.

Impacto negativo en la productividad y el ancho de banda

El uso de los medios sociales ha generado una disminución de la productividad y el ancho de banda de TI. Algunas organizaciones han respondido a esto aumentando el ancho de banda de Internet para adaptarse al mayor uso de los medios sociales en el lugar de trabajo.

Ataques de virus y malware

Los ataques de virus y malware han aumentado como consecuencia del uso de los medios sociales. Las tecnologías que los encuestados consideraron más importantes para reducir o mitigar las amenazas de los medios sociales son el antivirus/antimalware, el gateway web seguro (SWG) y la administración del acceso y la identidad.

La perspectiva mundial

Hay diferencias significativas en las prioridades, las percepciones y las reacciones de cada uno de los 12 países que participaron en la encuesta en relación con el uso y los riesgos de los medios sociales en el lugar de trabajo.

- **Percepción de riesgo**

Canadá, Hong Kong y México ven a los medios sociales con una seria amenaza, mientras que Francia e Italia son los menos propensos a ver a los medios sociales como una amenaza. Las organizaciones alemanas tienen la mayor confianza en su capacidad para hacer frente a las amenazas.

- **Los medios sociales son una herramienta importante para los negocios**
Las organizaciones del Reino Unido, México, India, Alemania y Hong Kong son las más propensas a considerar a los medios sociales importantes para cumplir con los objetivos empresariales. Italia, Australia y Brasil son menos propensos a ver la importancia de los medios sociales.
- **Políticas para administrar el uso de los medios sociales**
Alemania es también el único país donde la mayoría de los encuestados creen que tienen una política para administrar el uso aceptable o inaceptable de los medios sociales. En Italia, Singapur y Francia, las organizaciones son más propensas a creer que carecen de esta política.
- **Aumento del ancho de banda de Internet para apoyar el uso de los medios sociales**
Singapur, el Reino Unido, Canadá, Australia y Francia tienen el mayor porcentaje de organizaciones que invirtieron en ancho de banda para permitir el uso de los medios sociales..
- **Uso de los medios sociales con fines empresariales y no empresariales**
Las organizaciones de Alemania tienen el mayor uso de los medios sociales con fines empresariales, mientras que los Estados Unidos, el Reino Unido, Francia, Italia y México muestran un mayor uso de estos sitios para fines no empresariales. Alemania e India utilizan la menor cantidad de minutos para cuestiones personales.
- **Ataques de virus y malware como resultado del uso de los medios sociales**
Los encuestados en todos los países creen que sus organizaciones han sufrido un aumento de actividades de malware como resultado del uso de los medios sociales por parte de los empleados en el lugar de trabajo. El menor nivel de aumento de ataques de malware como resultado del uso de los medios sociales por parte de los empleados ocurrió en Hong Kong.

Recomendaciones

Los profesionales de TI y de seguridad de TI en todo el mundo reconocen el impacto positivo que los medios sociales están teniendo en la capacidad de sus organizaciones para comercializar y comunicar con eficacia. El desafío que enfrentan es asegurar que el uso de los medios sociales no ponga en peligro la seguridad de sus redes empresariales.

Reconocimiento del riesgo

Para poder entender y controlar los riesgos que presentan los medios sociales en el lugar de trabajo, las organizaciones deben considerar una evaluación de riesgos para entender qué prácticas pueden estar poniéndolos en riesgo. Es necesario informar a los empleados con claridad el impacto del uso que hacen de los medios sociales en la empresa. Será necesario implementar una política integral que atienda los riesgos y detalle los procedimientos de seguridad para todos los empleados y contratistas que utilizan las herramientas de los medios sociales en el lugar de trabajo.

Seguridad del contenido en tiempo real

Las organizaciones necesitan poder mejorar su capacidad para detectar y prevenir ataques. La Web social dinámica exige una defensa de seguridad de TI que va más allá de las tecnologías Web con políticas fijas y firmas, como los antivirus y firewalls, que ya no brindan una protección adecuada contra las amenazas. Deben considerar las ventajas de la seguridad de contenido en tiempo real que analiza la información en tiempo real a medida que esta se genera y se consume.

Controles de políticas para una mayor productividad

Los medios sociales incluyen video a pedido (VoD) y eventos de descarga en vivo que elevan el ancho de banda. Los problemas de productividad y ancho de banda se pueden solucionar aplicando límites de tiempo, administración de ancho de banda y orientación. Con estos controles, es posible permitir a los empleados disfrutar de la libertad de la Web social con controles de políticas para mantener la productividad y conservar el uso de los recursos en los niveles deseados.

Medios sociales: el desafío por venir

Se considera que las redes sociales tienen una importancia esencial en la capacidad de una organización para lograr sus objetivos empresariales – ayudan a crear mayor conciencia de la marca, mejorar la imagen y obtener inteligencia del público objetivo para ayudar a mejorar los productos y servicios..

A medida que la tecnología de medios sociales y la seguridad de estas herramientas continúan evolucionando, las organizaciones que han elegido un enfoque estratégico para entender, administrar y controlar los riesgos estarán en una posición más sólida para sacar provecho de los incuestionables beneficios que esta tecnología puede brindar.



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.

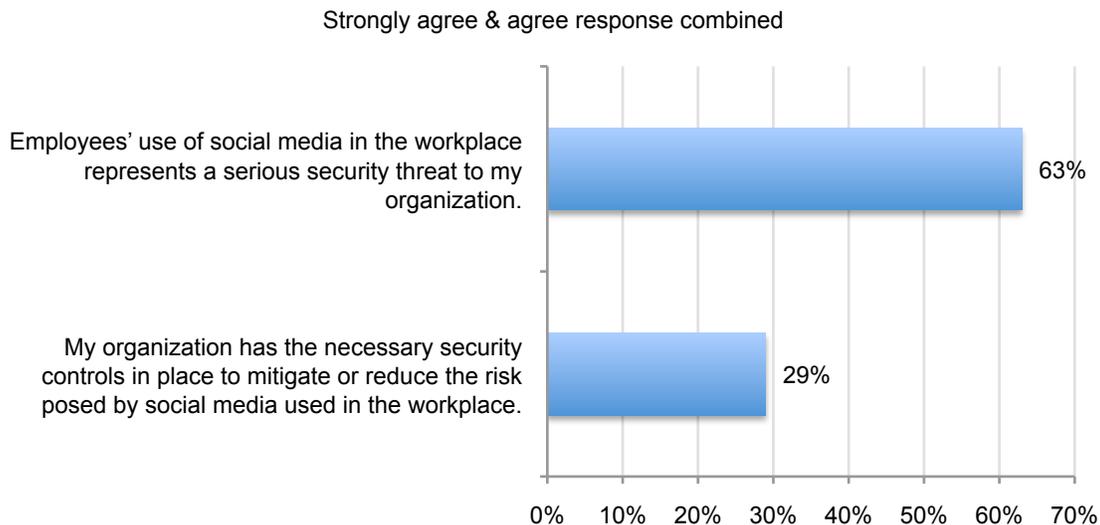
Part 2. Analysis of key findings

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.

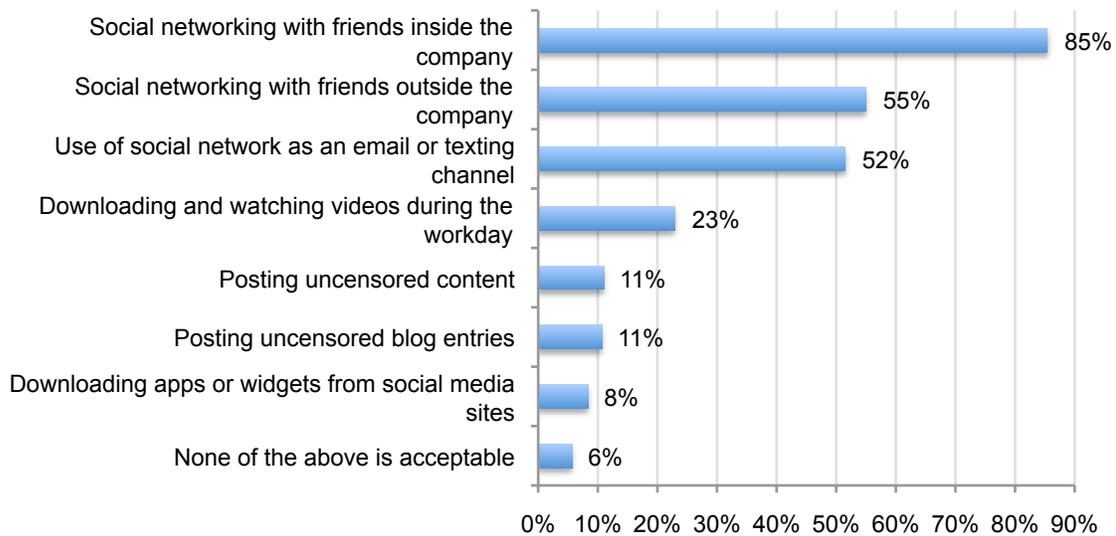


If there is a policy to address the acceptable use of social media in the workplace, 65 percent say their organizations do not enforce it or they are unsure. The top three reasons for not enforcing these policies are lack of governance and oversight (44 percent), other security issues are a priority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

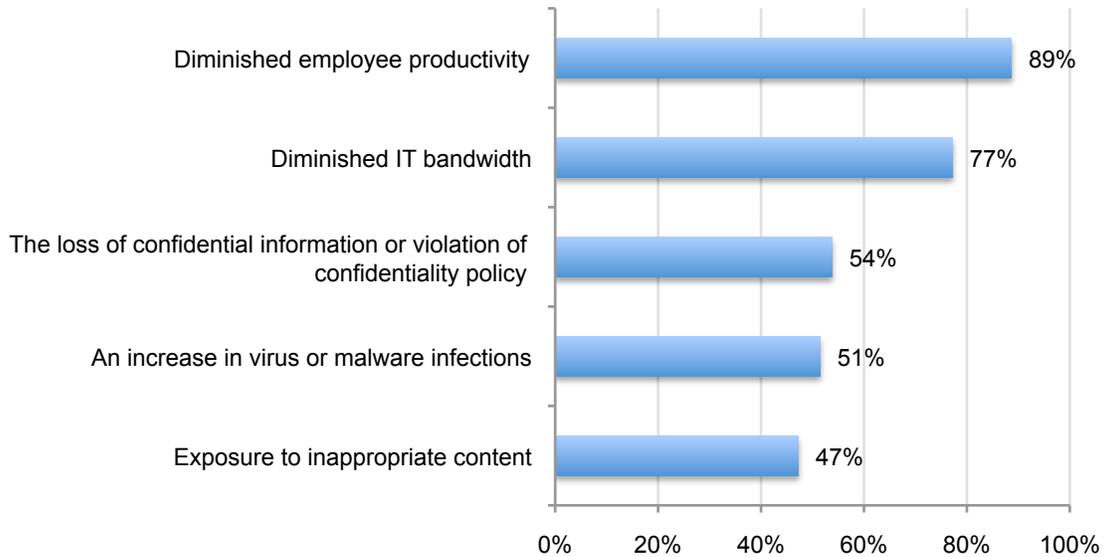
Bar Chart 2: What is considered the acceptable use of social media in the workplace



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

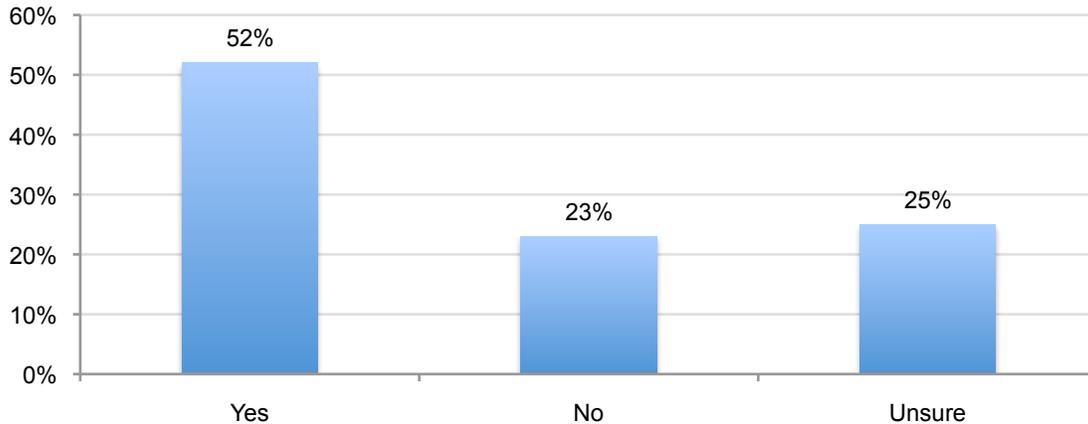
Each bar represents the percent of respondents who said the issue has already happened or is very likely to occur.



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.

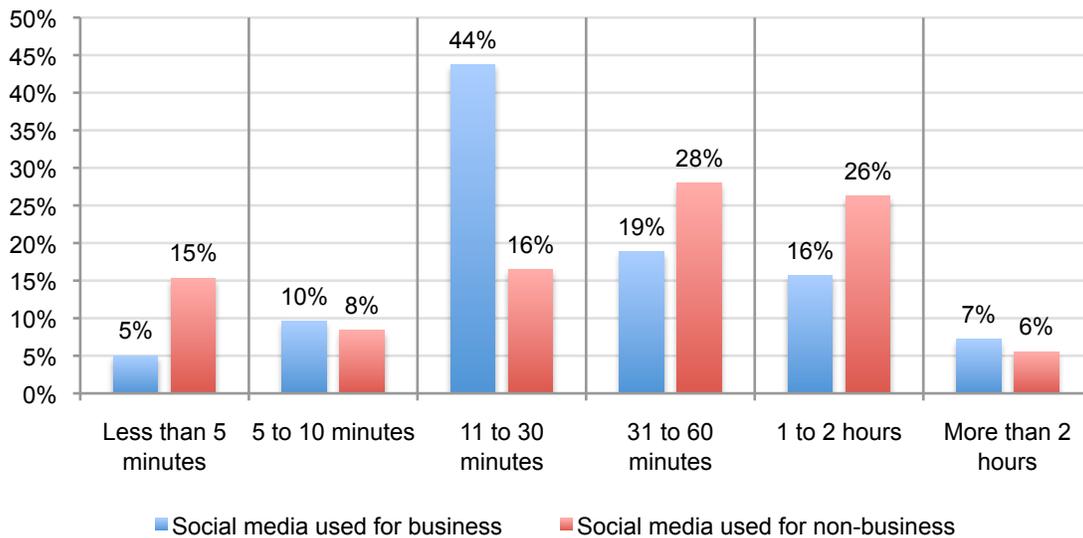
Bar Chart 4: Did your organization experience any increase in virus and malware attacks as a result of employees' use of social media in the workplace?



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.

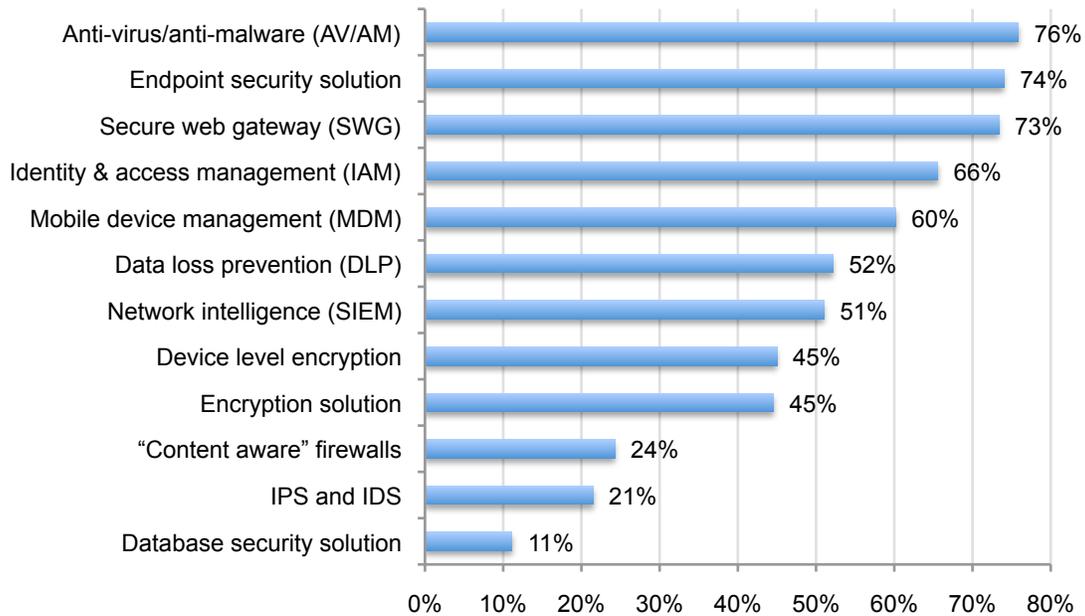
Bar Chart 5: Approximate time spent by employees on social media during the workday



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.

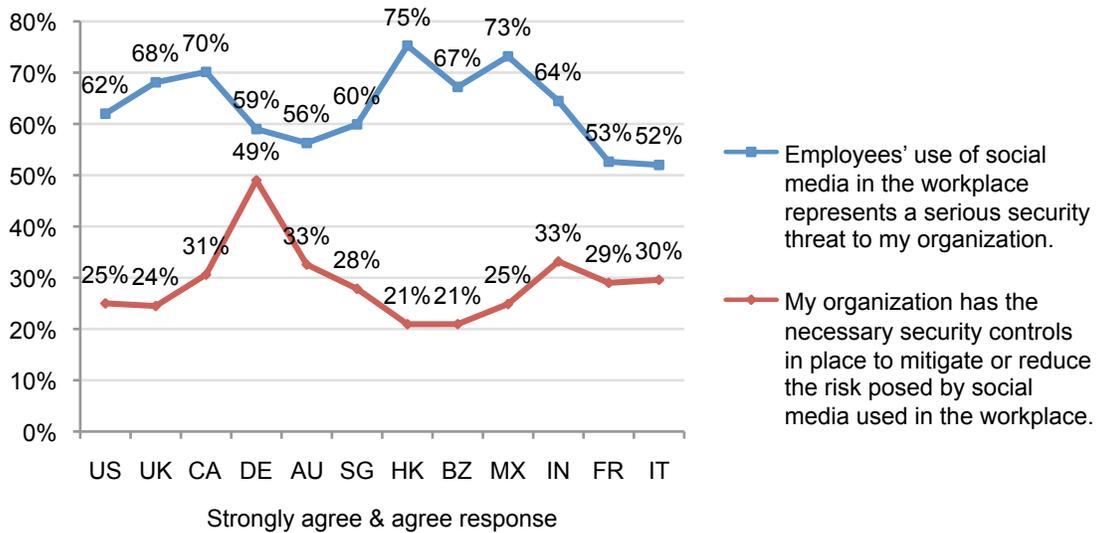
Part 3. Most significant country differences

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

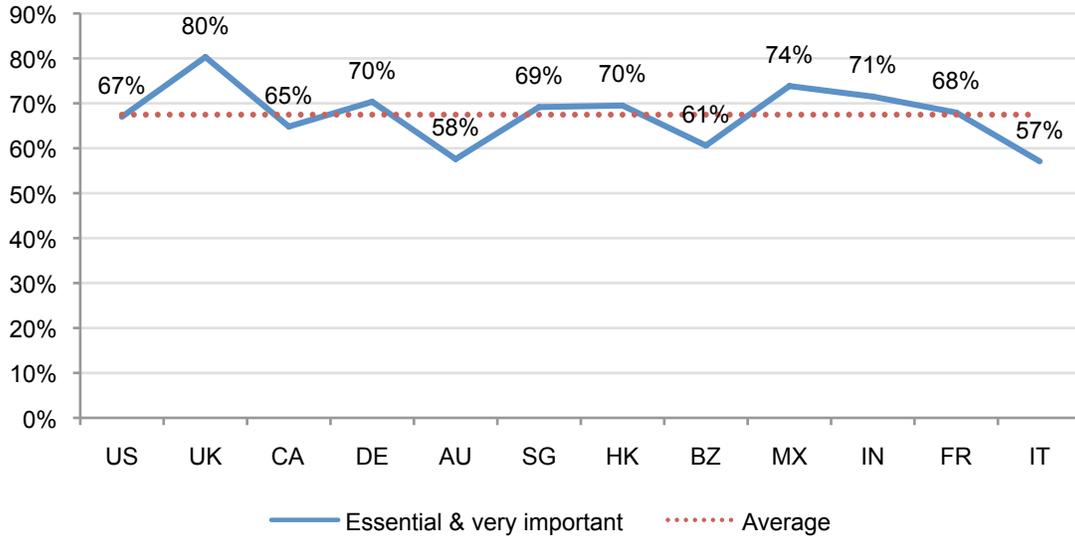


² The horizontal axis to each line graph represents the individual country sample. See Table 1 (Methods section) for country legend used in this section.

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?

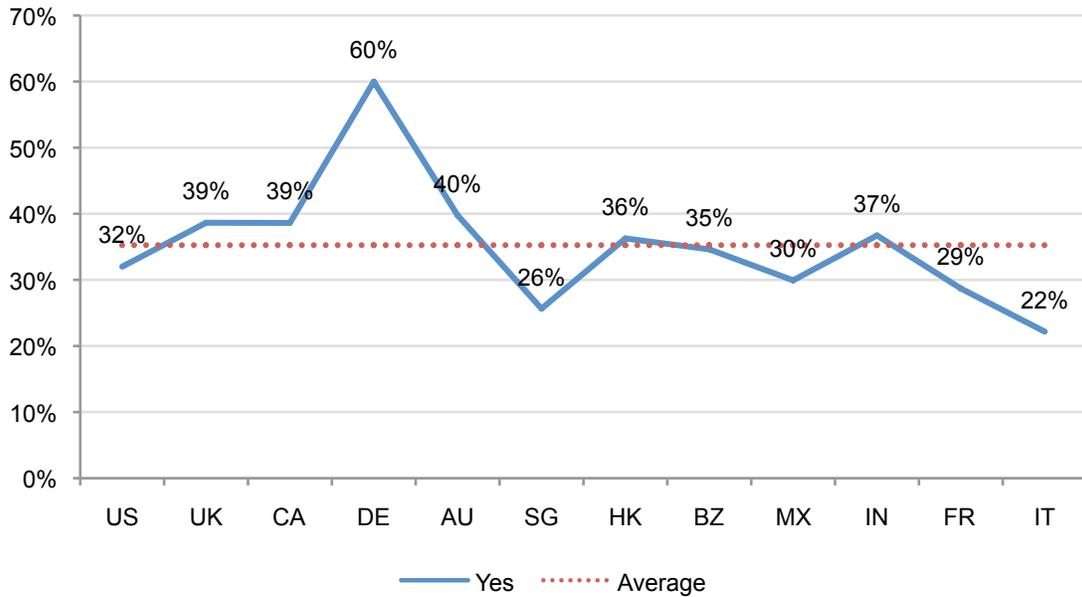
Results shown for 12 separate country samples



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?

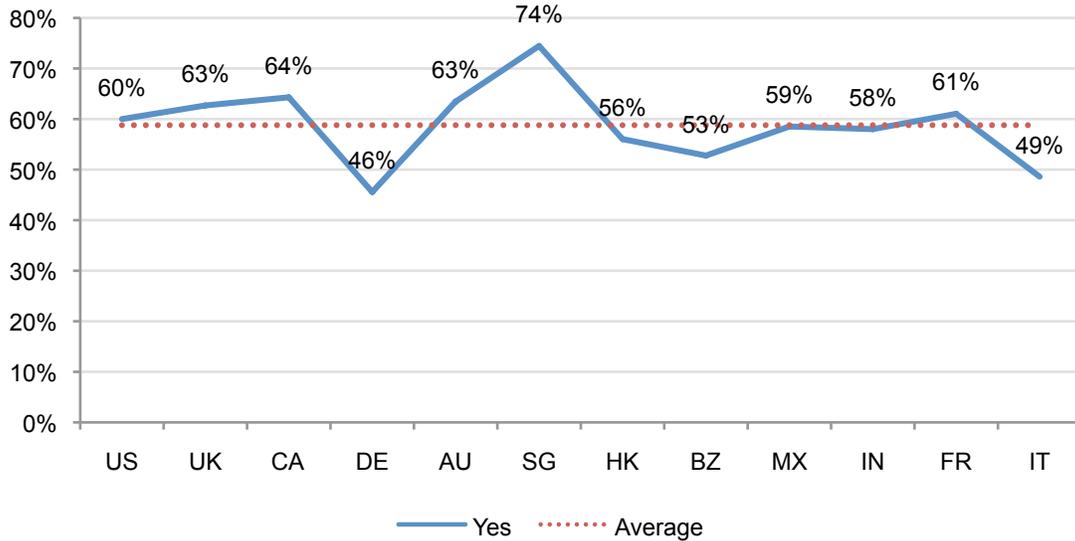
Results shown for 12 separate country samples



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?

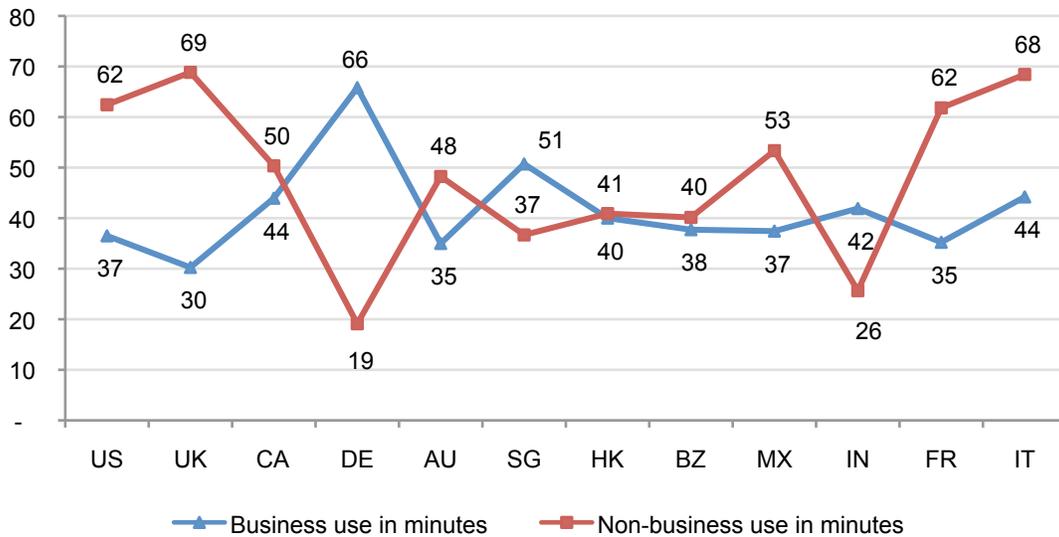
Results shown for 12 separate country samples



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

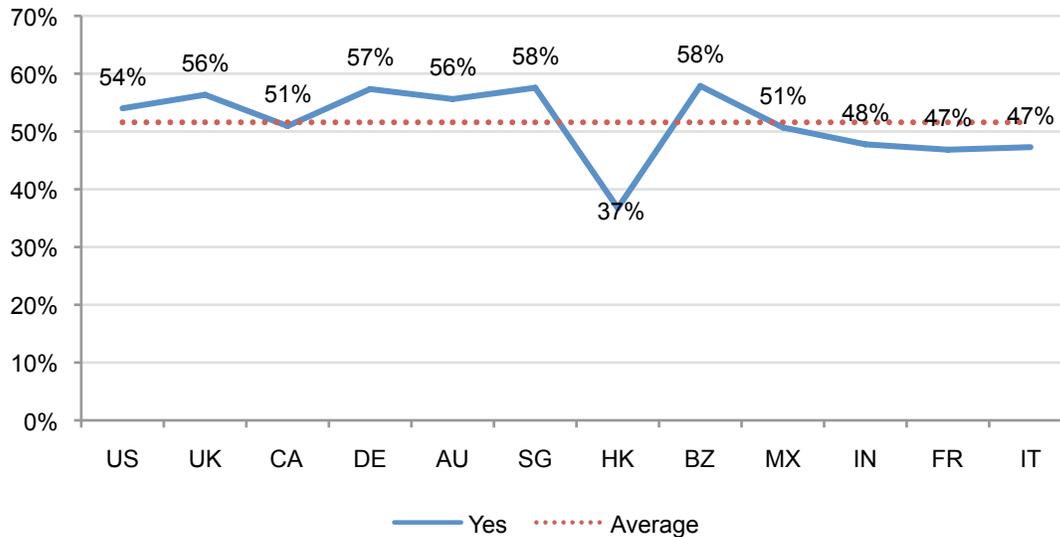
Results shown for 12 separate country samples



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

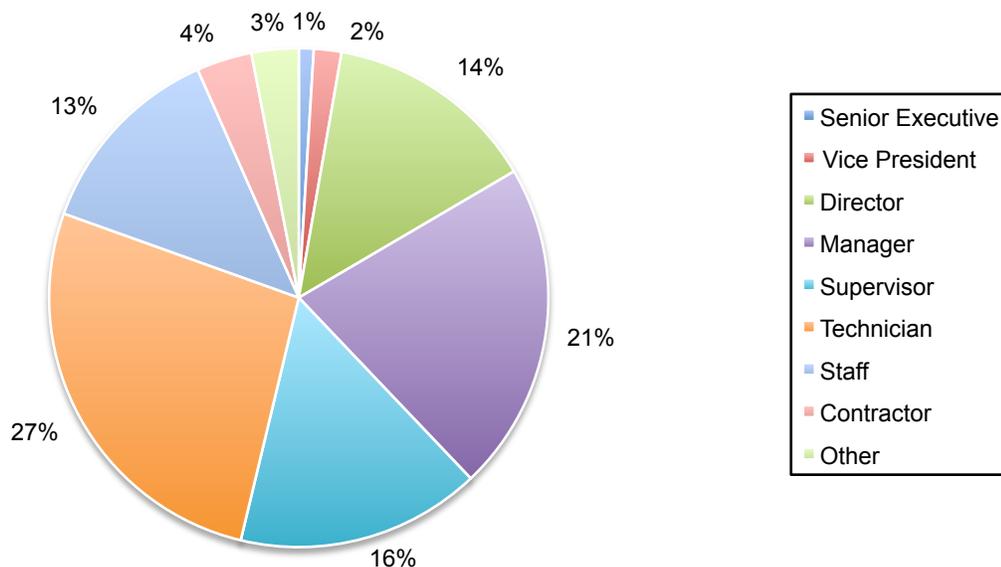
Table 4 reports the sample response for 12 separate country samples. The sample response for this study conducted over a 30-day period ending in July 2011. Our consolidated sampling frame of practitioners in 12 countries consisted of 116,491 individuals who have bona fide credentials in the IT or IT 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.

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.

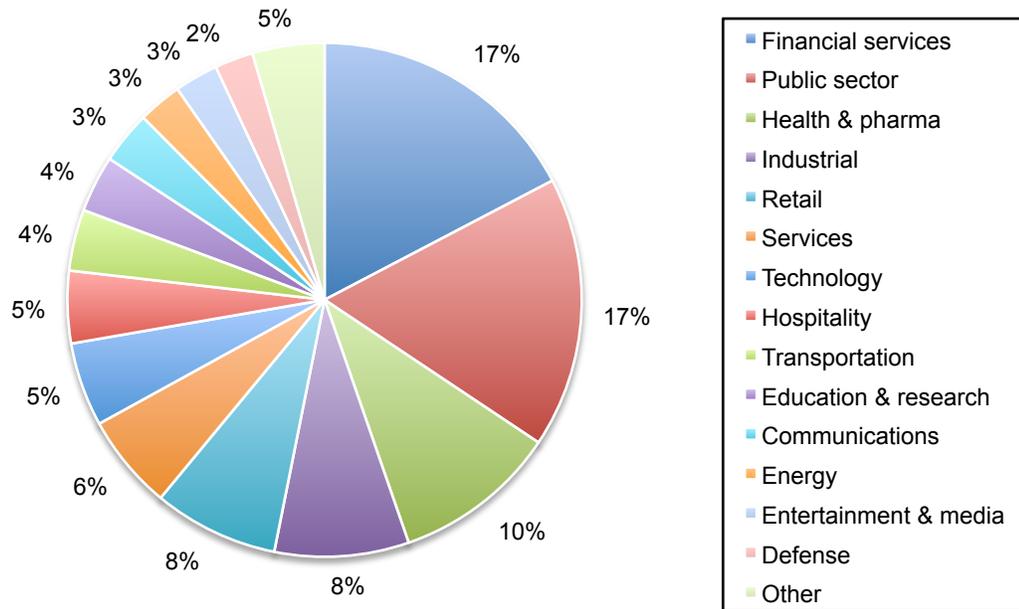
Pie Chart 1: Distribution of respondents according to position level

Consolidated for 12 separate country samples



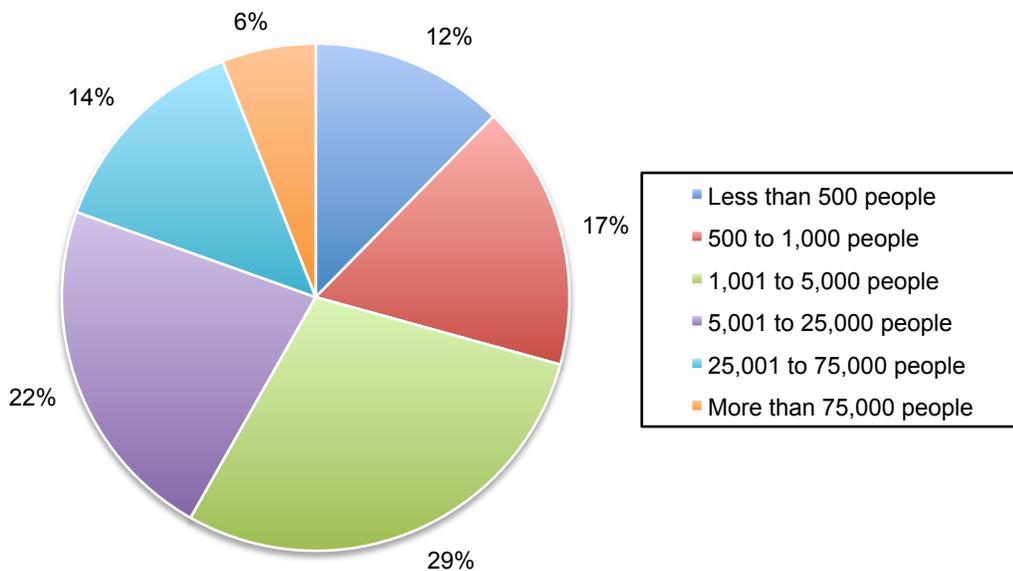
Pie Chart 2 reports the respondents' organizations primary industry segments. As shown, 17 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 17 percent are located in public sector organizations,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