Web 2.0 Security in the Workplace

Study of IT practitioners in the United States, United Kingdom, Australia, France & Japan

Sponsored by Check Point

Independently conducted by Ponemon Institute LLC

Publication Date: 1 June, 2010

Web 2.0 Security in the Workplace

Study of IT Practitioners in the United States, United Kingdom, Australia, France and Japan

I. Executive Summary

Ponemon Institute and Check Point are pleased to present the results of *Web 2.0 Security in the Workplace*. The present global study involves an expert panel of IT and IT security practitioners located in the United States (US), United Kingdom (UK), Australia (AU), France (FR), and Japan (JP). The objective of the study is to understand:

- What IT and IT security practitioners think about the threat of Web 2.0 use in the workplace.
- Who should be held most responsible for dealing with Web 2.0 security risks.
- How much of a priority is the mitigation of threats caused by employees' when using Web 2.0 apps such as social networks, social messaging, blogs and wikis.

Web 2.0 creates nearly unlimited opportunities for human collaboration. Internet tools such as social networking, blogs, search engines and wikis connect people who have shared interests, beliefs and values. Despite the real benefits created by Web 2.0 applications, there are inherent risks associated with their use such as workplace inefficiencies, malware, data loss and viruses.

This study is important because it demonstrates how the misuse of Web 2.0 applications by a company's employees can put the organization at risk. According to our annual cost of a data breach study, insider negligence is a major cause of data loss. In the UK, insider negligence accounts for 46 percent of all data breach incidents. In the US, it is 40 percent, in France 35 percent, and in Australia it is 35 percent.[1]

In another recent study, we found that 70 percent of IT practitioners from US-based multinationals do not think their organizations allocate sufficient resources to secure and protect critical website applications.[2] We believe insider threats coupled with web applications not being adequately secured create a perfect storm for a data loss disaster.

We surveyed more than 2,100 individuals located in five countries. Participants were asked to respond to six objectively framed questions.[3] Following are our most salient findings:

- **Many respondents believe their organization's employees (a.k.a. end-users) do not consider security issues when downloading Internet applications, opening links, and web browsing on their office computers.** Fifty-two percent of US, 49 percent of UK and 48 percent of Australian respondents, respectively, believe end-users <u>rarely or never</u> consider security issues in their daily business communications. In contrast, only 22 percent of respondents in France and 24 percent in Japan believes end-users rarely or never considers security issues when using Internet applications.
- **Respondents are unclear about who should be held most responsible for ensuring the safe use of Internet applications in the workplace.** According to more than half of respondents in the US, UK and Australia, the most responsible party for minimizing Web 2.0 security risk <u>should be</u> the end-user, followed by information security (CISO) and corporate IT (CIO). In contrast, respondents in France believe human resources, followed by information security, are most responsible for minimizing security risk in the Web 2.0 environment. In Japan, legal followed by corporate IT are viewed as the most responsible parties for ensuring safety and security when using of Web 2.0 apps.

[1] 2009 Annual Study: Global Cost of a Data Breach. Ponemon Institute, April 2010.
[2] State of Web Application Security. Ponemon Institute April 2010.
[3] The present survey questions were part of a larger omnibus survey instrument (a.k.a. Meta survey) fielded on a quarterly cycle in all five countries.

- **A majority of respondents in the US and Japan believe Web 2.0 applications interfere with the security posture of their companies.** Eighty-two percent of respondents in Japan and 80 percent in the US believe Web 2.0 applications have a significant or very significant impact on their companies' security posture. In both the UK and Australia, 58 percent believe this to be the case. In France, the level of concern appears to be much lower at 45 percent.
- **Workplace inefficiencies, malware, data loss and viruses are the top four threats caused by the insecure use of Web 2.0.** Respondents in the US, UK and Australia cite workplace inefficiencies as the number one threat, followed by malware, data loss and viruses. Among French and Japanese respondents, the number one threat concerns virus infection. Japanese respondents are much more concerned about botnets than respondents in other countries.
- **Minimizing Web 2.0 security risk is a very high or high priority for US and Japanese respondents.** Both US and Japanese respondents have a higher sense of urgency in terms of resolving extant security risks immediately. In contrast, many respondents in Australia and UK do not see securing Web 2.0 as an urgent priority and, hence, can be addressed over the next two to five years. Finally, 63 percent of French respondents say Web 2.0 is a low priority security threat.

II. Key Findings

In this section, we provide the summarized findings expressed as percentage frequencies in tabular form. In addition, results are provided in line graphs, bar charts, and pie charts to exemplify our most salient results.

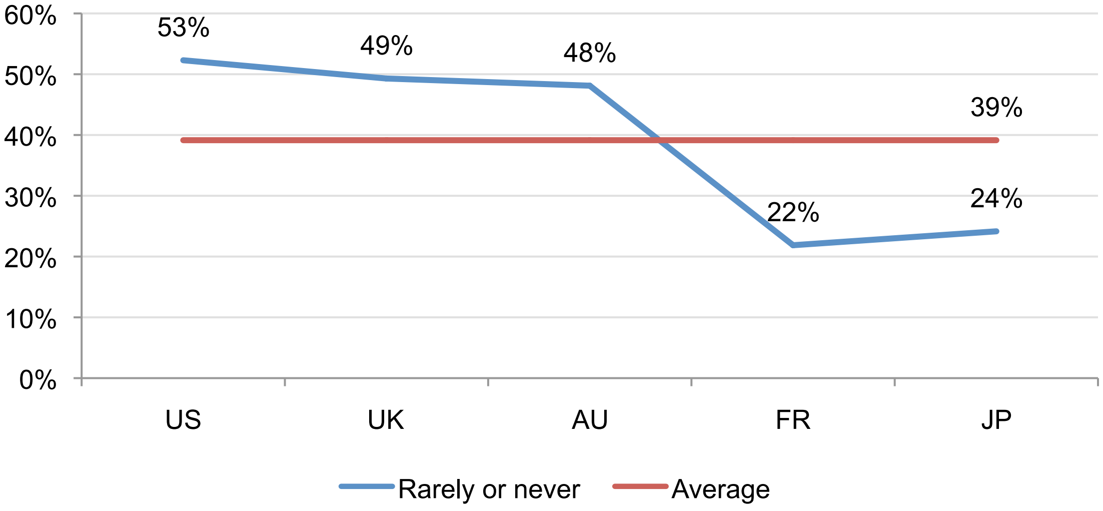
1. Many respondents believe their organization's employees (a.k.a. end-users) do not consider security issues when downloading Internet applications, opening links, and web browsing on their office computers.

Table 1 reports respondents' perceptions about the security consciousness of end-users in their organizations when using Internet applications in the workplace. Viewing Table 1, it is clear that only a small number of respondents in all five countries believe end-users consider security issues in their daily business communications. In addition, there are significant differences among countries, wherein respondents in the US, UK and Australian hold more negative views about the security consciousness of end-users than respondents in France and Japan.

Table 1 Do end-users consider security issues in their daily business communications—for example, when downloading Internet apps, opening links, web browsing on their office computers, etc.?	US	UK	AU	FR	JP	Average
All the time	11%	12%	11%	27%	25%	17%
Most of the time	16%	18%	18%	21%	15%	18%
Some of the time	21%	20%	23%	30%	36%	26%
Rarely	38%	35%	37%	10%	13%	27%
Never	15%	14%	11%	12%	11%	13%
Total	100%	100%	100%	100%	100%	100%

Line Graph 1 reports the rarely and never response combined for five countries. As shown, US respondents hold the most unfavorable view about end-user security consciousness (53 percent), followed by the UK (49 percent) and Australia (48 percent).
Respondents in France (22 percent) and Japan (24 percent) hold a more favorable view about end-user security consciousness.

Line Graph 1
Do end-users consider security issues in their daily business communications?



2. Respondents are unclear about who should be held most responsible for ensuring the safe use of Internet applications in the workplace.

Table 2 reports the results of a question requiring respondents to rank five functions in terms of who should be held most responsible for ensuring safe uses of Web 2.0 applications. Both the average rank and rank order are reported. It is interesting to see the nearly identical rank order provided by US, UK and Australian respondents, where end-users are viewed as the most responsible and human resources as least responsible for ensuring security. Respondents in France and Japan do not view the end-user as being most responsible for preventing security risk. In contrast, respondents in France view human resources as most responsible, while Japanese respondents view their company's legal department as most responsible.

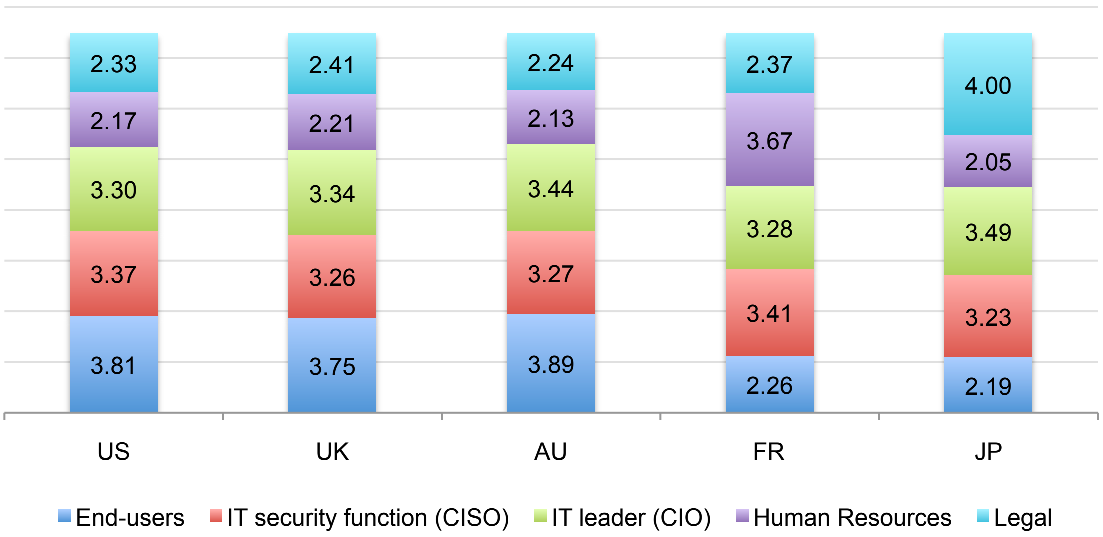
Table 2
Who **should be** most responsible for ensuring end-users' use of Internet applications and content sharing do not increase security risk for the organization? Ranking from 1 = most to 5 = least responsible

Q2: **AVERAGE RANK**	US	UK	AU	FR	JP	Average
End-users	2.19	2.25	2.11	3.74	3.81	2.82
IT security function (CISO)	2.63	2.74	2.73	2.59	2.77	2.69
IT leader (CIO)	2.70	2.66	2.56	2.72	2.51	2.63
Human Resources	3.83	3.79	3.87	2.33	3.95	3.55
Legal	3.67	3.59	3.76	3.63	2.00	3.33

Q2: **RANK ORDER**	US	UK	AU	FR	JP	Average
End-users	1	1	1	5	4	2.40
IT security function (CISO)	2	3	3	2	3	2.60
IT leader (CIO)	3	2	2	3	2	2.40
Human Resources	5	5	5	1	5	4.20
Legal	4	4	4	4	1	3.40

Bar Chart 1 provides the average rank transformed from high to low (where five equals the most important role). This chart shows that general consistency among respondents in the US, UK and Australia. It also shows that respondents in France and Japan hold different perceptions, especially about the role of end-users – perhaps suggesting cultural differences.

Bar Chart 1
The most responsible for ensuring end-users' safe use of Internet content
Average rank where 5 = most important and 1 = least important (rank transformed)



3. A majority of respondents in the US and Japan believe Web 2.0 applications interfere with the security posture of their companies.

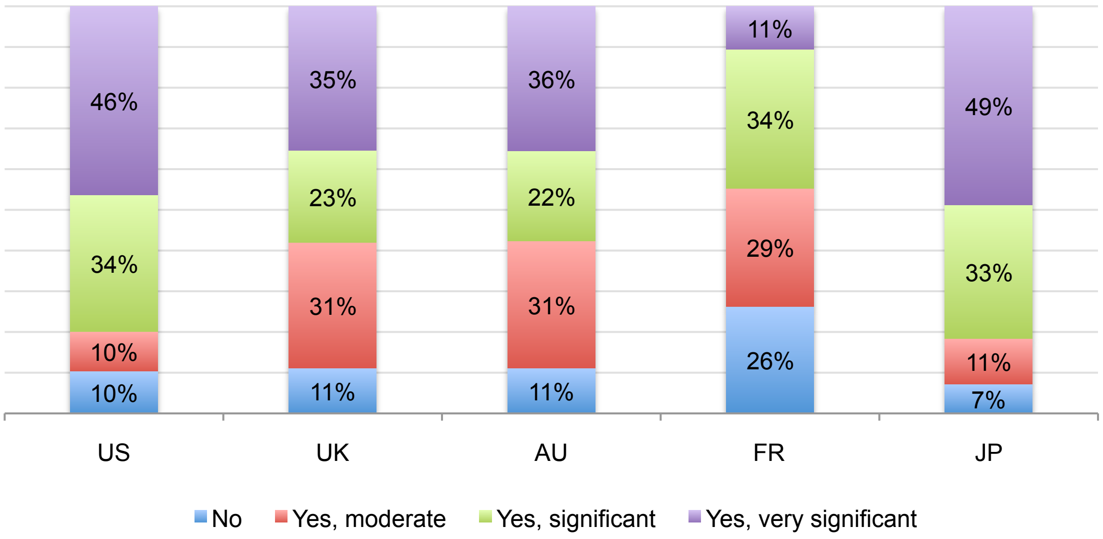
Table 3 reports the results for one survey question about whether Web 2.0 applications interfere with the security posture of respondents' organizations. As can be seen, an overwhelming majority of respondents in all five countries acknowledge that Web 2.0 applications interfere – at least have a moderate impact – on their organization's security posture. Respondents in Japan (49 percent) and the US (46 percent) are most likely to see Web 2.0 as having a very significant impact on their companies' security posture. Whereas respondents in France are least likely to see Web 2.0 as causing a very significant security risk.

Respondents from the UK and Australia hold very similar perceptions about the impact of Web 2.0 of their organizations' security posture. Accordingly, a majority of these respondents believe that Web 2.0 has a significant or very significant impact on the security posture of their companies (58 percent).

Table 3 Do Web 2.0 applications interfere with the security posture of your company?	US	UK	AU	FR	JP	Average
No	10%	11%	11%	26%	7%	13%
Yes, moderate impact	10%	31%	31%	29%	11%	22%
Yes, significant impact	34%	23%	22%	34%	33%	29%
Yes, very significant impact	46%	35%	36%	11%	49%	35%
Total	100%	100%	100%	100%	100%	100%

Bar Chart 2 provides a graphical representation of the percentage frequency data provided in the above table. It clearly shows the greatest variation in responses in the category "very significant impact" from a high yes response of 49 percent Japan to a low of 11 percent for France. Inversely, variation in the category "no impact" response ranges from a low of 7 percent for Japan to a high of 26 percent in France. These results suggest respondents in France are less concerned about the insecure use of Web 2.0 applications than respondents in other countries.

Bar Chart 2
Do Web 2.0 applications interfere with the security posture of your company?



4. Workplace inefficiencies, malware, data loss and viruses are the top three threats caused by the insecure use of Web 2.0 applications.

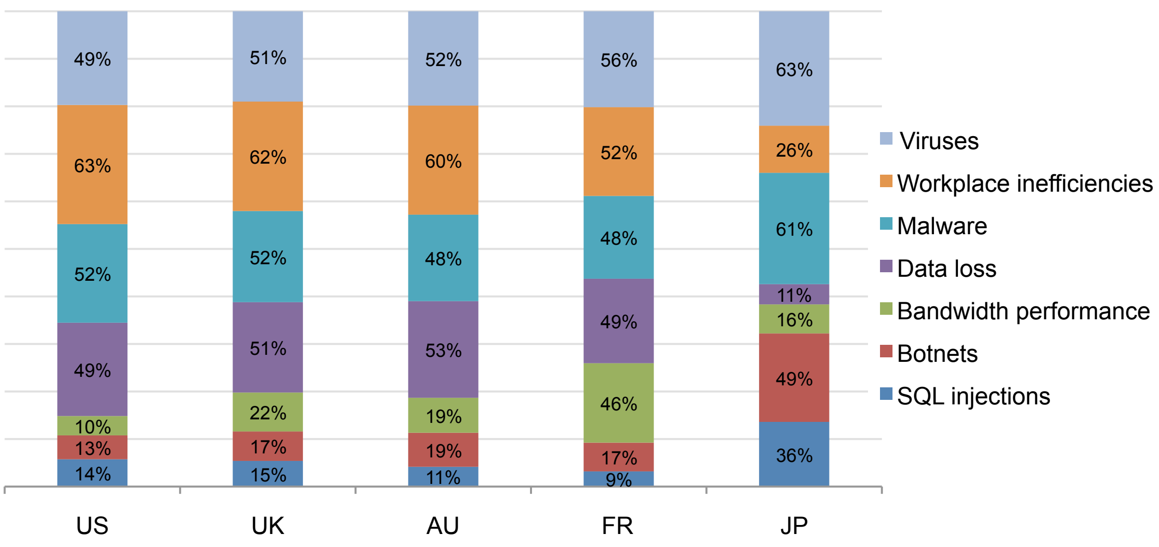
Table 4 reports the types of threats that the use of Web 2.0 applications introduces into the workplace. Overall, the number one threat concerns viruses (average at 54 percent), workplace inefficiencies (average at 53 percent), and malware (average at 52 percent). The least significant threats concern SQL injection (average at 17 percent) and bandwidth performance (average at 23 percent).

Table 4 What threats or problems do Web 2.0 applications cause when downloaded and used?	US	UK	AU	FR	JP	Average
Viruses	49%	51%	52%	56%	63%	54%
Workplace inefficiencies	63%	62%	60%	52%	26%	53%
Malware	52%	52%	48%	48%	61%	52%
Data loss	49%	51%	53%	49%	11%	43%
Botnets	13%	17%	19%	17%	49%	23%
Bandwidth performance	10%	22%	19%	46%	16%	23%
SQL injections	14%	15%	11%	9%	36%	17%

Bar Chart 3 provides a graphical representation of the above percentage frequency table. It reveals several significant differences among respondents in different countries. Accordingly, respondents in the US (63 percent), UK (62 percent) and Australia (60 percent) cite workplace inefficiencies as the number one threat vector, followed by malware, data loss and viruses.

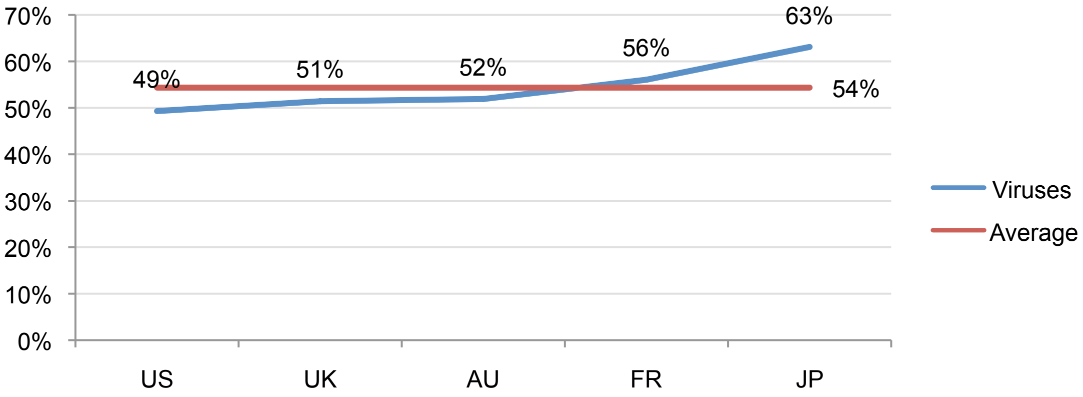
Among respondents in France and Japan respondents, the number one threat concerns virus infection (56 percent and 63 percent, respectively). Clearly, respondents in Japan appear to be more concerned about botnet attacks (49 percent) than respondents in all other countries. In contrast, respondents in Japan appear to be least concerned about data loss (16 percent).

Bar Chart 3
What threats do Web 2.0 applications introduce?

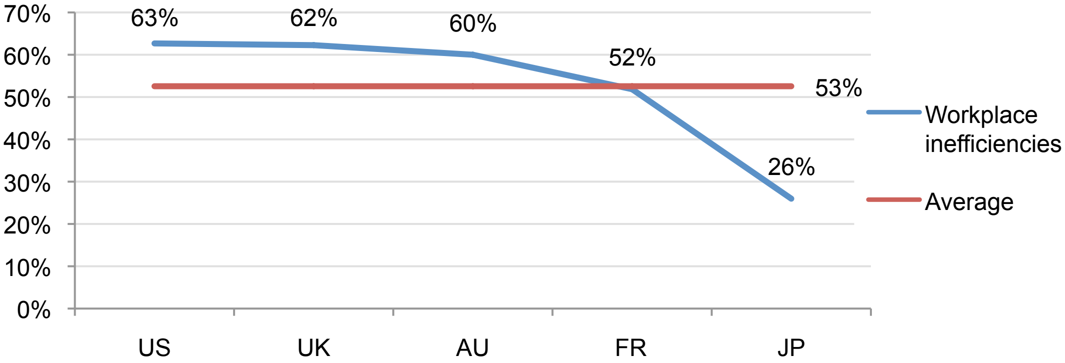


The following line graphs illustrate the variation in three perceived Web 2.0 security threats – namely, viruses, workplace inefficiencies and botnets – across all five countries surveyed in our research.

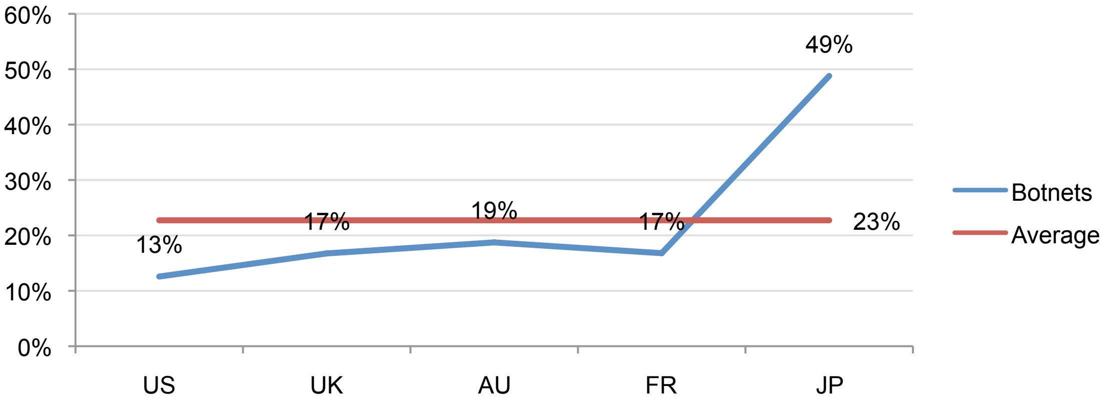
Line Graph 2a
Virus threats introduced by Web 2.0 applications



Line Graph 2b
Workplace inefficiencies introduced by Web 2.0 application



Line Graph 2c
Botnets introduced by Web 2.0 applications



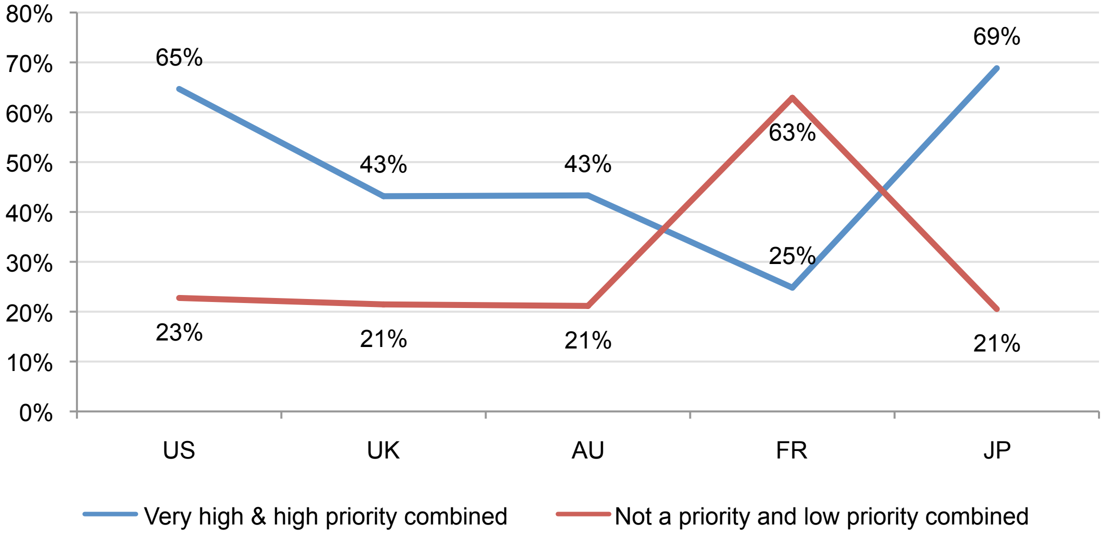
5. Minimizing Web 2.0 security risk is a very high or high priority, especially for respondents in the US and Japan.

Table 5 reports the summarized responses to the question concerning the priority level of Web 2.0 application security in respondents' organizations. On average, we see that 49 percent of respondents rate this as either a high or very high priority.

Table 5 Where on your list of security priorities does protecting your company against risks associated with Web 2.0 applications fall?	US	UK	AU	FR	JP	Average
Very high priority	32%	10%	11%	13%	37%	21%
High priority	33%	33%	32%	12%	31%	28%
Medium priority	13%	35%	36%	12%	11%	21%
Low priority	11%	9%	12%	42%	9%	17%
Not a priority	12%	12%	9%	21%	12%	13%
Total	100%	100%	100%	100%	100%	100%

Line Graph 3 shows significant variation in responses across countries. Specifically, respondents from the US (65 percent) and Japan (69 percent) are more likely to rate this security risk at a very high or high priority level than respondents in the UK (43 percent), Australia (43 percent) and France (25 percent). In contrast, respondents in France are more likely to rate Web 2.0 security risk at a lower priority level or not a priority (63 percent) than all other countries (21 percent).

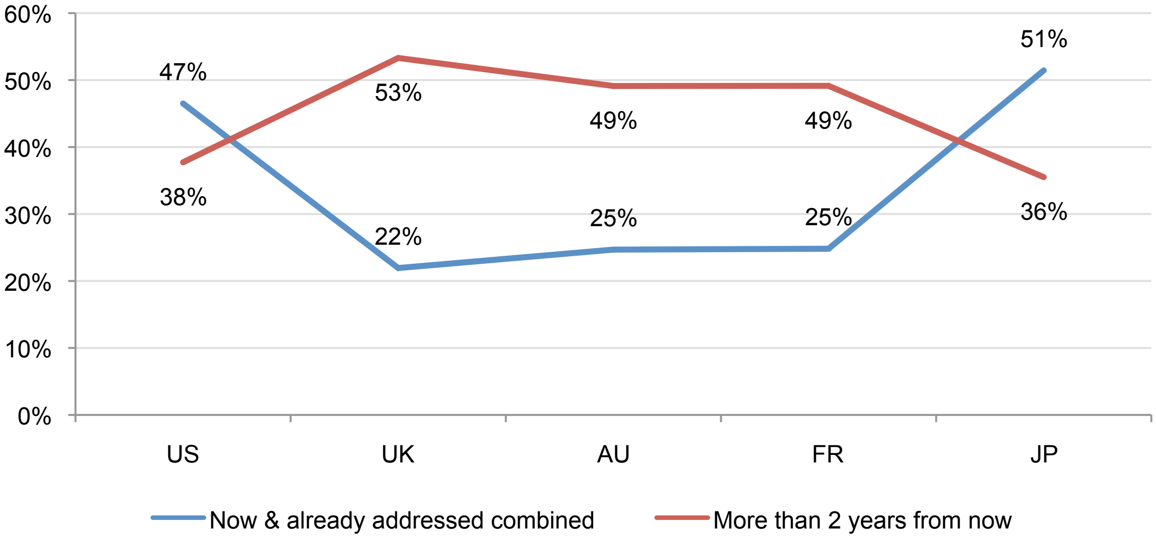
Line Graph 3
Is Web 2.0 security risk a priority?



Respondents were asked to respond to a related question about the anticipated timeline for addressing Web 2.0 security risks (from already addressed to never). Table 6 and Line Graph 3 both reveal that respondents in the US and Japan have a higher sense of urgency in terms of resolving Web 2.0 security risks than respondents in all other countries. In contrast, respondents in Australia and UK do not see securing Web 2.0 as an urgent priority and, hence, they believe it can be addressed over a longer timeframe (for instance, the next two to five years). Finally, many French respondents believe Web 2.0 is a low priority security threat that has already been addressed within their organizations.

Table 6 When do you plan to address the security of Web 2.0 applications?	US	UK	AU	FR	JP	Average
Now	36%	11%	13%	15%	31%	21%
1-2 years	16%	25%	26%	26%	13%	21%
2-5 years	29%	43%	38%	40%	27%	35%
5-7 years	2%	2%	4%	3%	3%	3%
More than 7 years	2%	3%	3%	2%	3%	3%
Already addressed	10%	11%	12%	10%	21%	13%
Never	6%	6%	4%	4%	3%	5%
Total	100%	100%	100%	100%	100%	100%

Line Graph 4
When do you plan to address the security of Web 2.0 applications



III. Methods

Five national sampling frames consisting of nearly 46,000 adult-aged individuals who reside the US, UK, Australia, France or Japan were used to recruit and select participants to this survey. Our omnibus sampling frames were built from several proprietary lists of experienced IT and IT security practitioners. In total, 2,412 respondents completed the survey. Of the returned instruments, 269 surveys failed reliability checks. A total of 2,143 surveys were used as our final Meta sample, which represents a 4.7 percent response rate.

Table 7 Sample response	US	UK	AU	FR	JP	Total
Total sampling frame	11833	8995	6517	8049	10502	45896
Invitations sent	10568	7553	6021	7480	9009	40631
Responses	555	476	433	486	462	2412
Rejections	54	52	36	79	48	269
Final sample	501	424	397	407	414	2143
Response rate	4.2%	4.7%	6.1%	5.1%	3.9%	4.7%

Pie Chart 1 reports the primary industry sector of respondents' organizations for all five-country samples combined. As shown, the largest segments include financial services, industrial, government, services, retail, and services.

Pie Chart 1: Industry distribution of respondents' organizations

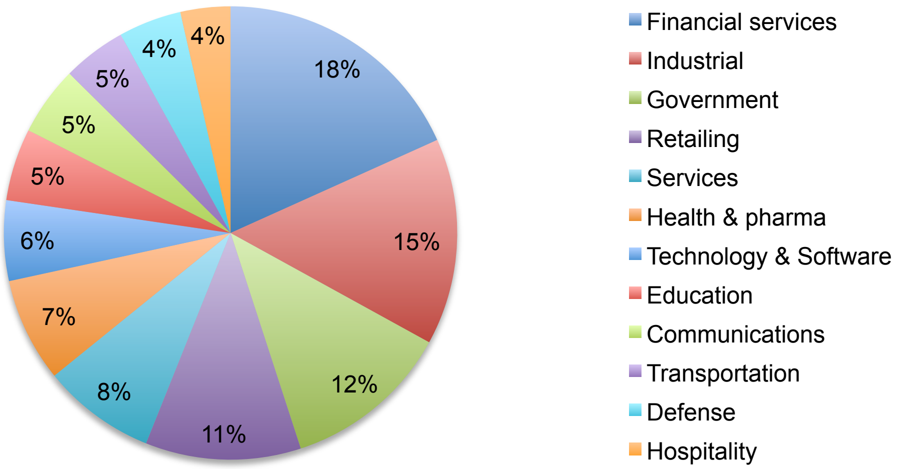


Table 8 reports the respondent organization's global headcount. As shown, 66 percent of respondents work within companies with more than 1,000 employees. More than 39 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 8 Worldwide headcount of respondents' companies	US	UK	AU	FR	JP	Average
Less than 500 people	11%	18%	21%	19%	16%	17%
500 to 1,000 people	13%	14%	22%	20%	15%	17%
1,001 to 5,000 people	26%	32%	28%	27%	23%	27%
5,001 to 25,000 people	27%	16%	23%	21%	25%	22%
25,001 to 75,000 people	13%	16%	4%	8%	14%	11%
More than 75,000 people	10%	4%	2%	5%	7%	6%
Total	100%	100%	100%	100%	100%	100%

Table 9 reports the respondent's primary reporting channel. Overall, 69 percent of respondents are located in the organization's IT department (led by the company's CIO or CTO).

Table 9 Respondents' reporting channels.	US	UK	AU	FR	JP	Average
Chief information officer	53%	60%	61%	55%	70%	60%
Chief technology officer	10%	8%	8%	9%	10%	9%
Chief information security officer	16%	9%	11%	12%	8%	11%
Chief security offer	6%	5%	3%	4%	5%	5%
Chief financial officer	3%	4%	3%	6%	0%	3%
Compliance Officer	2%	3%	4%	0%	0%	2%
Human Resources VP	1%	0%	4%	5%	0%	2%
Chief risk officer	6%	5%	5%	3%	3%	4%
Other	3%	6%	1%	6%	4%	4%
Total	100%	100%	100%	100%	100%	100%

Table 10 reports the respondents' position level. As can be seen, a majority of respondents self-report their positions at or above the supervisory level.

Table 10 Respondents' position level	US	UK	AU	FR	JP	Average
Senior Executive	0%	2%	1%	1%	1%	1%
Vice President	1%	0%	2%	0%	0%	1%
Director	15%	7%	10%	6%	8%	9%
Manager	19%	21%	15%	20%	21%	19%
Supervisor	17%	24%	28%	24%	24%	24%
Technician	28%	30%	32%	30%	32%	30%
Staff	13%	6%	0%	7%	1%	6%
Contractor	5%	5%	8%	12%	12%	8%
Other	3%	4%	4%	0%	2%	2%
Total	100%	100%	100%	100%	100%	100%

Overall, the sample consisted of individuals who hold full-time employment in the IT or a related field. The median and median experience level in IT or IT security for the combined samples are 9.42 and 9.50, respectively. Approximately, 28 percent of respondents are female and 72 percent male. Please note that this skewed result on gender is consistent with other global studies of IT and IT security practitioners. Other facts about this sample are provided in the Appendix to this report.

IV. Caveats

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 individuals, 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 instrument.

- 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. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used an omnibus collection method, it is possible that responses are biased by other items contained in the Meta survey instrument.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix I: Survey Question Details

Fieldwork concluded on April 16, 2010

Sample response	US	UK	AU	FR	JP	Total
Total sampling frame	11833	8995	6517	8049	10502	45896
Invitations sent	10568	7553	6021	7480	9009	40631
Responses	555	476	433	486	462	2412
Rejections	54	52	36	79	48	269
Final sample	501	424	397	407	414	2143
Response rate	4.2%	4.7%	6.1%	5.1%	3.9%	4.7%

Q1: In your opinion, do end-users consider security issues in their daily business communications—for example, when downloading Internet applications, opening links, web browsing on their office computers, etc.?	US	UK	AU	FR	JP	Avg
All the time	11%	12%	11%	27%	25%	17%
Most of the time	16%	18%	18%	21%	15%	18%
Some of the time	21%	20%	23%	30%	36%	26%
Rarely	38%	35%	37%	10%	13%	27%
Never	15%	14%	11%	12%	11%	13%
Total	100%	100%	100%	100%	100%	100%

Q2: Who **should be** most responsible for ensuring end-users' use of Internet applications and content sharing do not increase security risk for the organization?

United States	1	2	3	4	5	Avg Rank
End-users	54%	17%	4%	7%	18%	2.19
IT security function (CISO)	17%	37%	21%	16%	9%	2.63
IT leader (CIO)	16%	17%	53%	9%	5%	2.70
Human Resources	4%	14%	7%	44%	31%	3.83
Legal	9%	15%	12%	26%	37%	3.67

United Kingdom	1	2	3	4	5	Avg Rank
End-users	54%	15%	4%	7%	21%	2.25
IT security function (CISO)	16%	17%	50%	10%	6%	2.74
IT leader (CIO)	15%	37%	23%	16%	8%	2.66
Human Resources	4%	15%	8%	44%	29%	3.79
Legal	10%	17%	13%	25%	35%	3.59

Australia	1	2	3	4	5	Avg Rank
End-users	55%	19%	4%	7%	16%	2.11
IT security function (CISO)	14%	22%	45%	13%	6%	2.73
IT leader (CIO)	18%	34%	30%	11%	7%	2.56
Human Resources	5%	12%	6%	46%	32%	3.87
Legal	8%	14%	12%	27%	39%	3.76

France	1	2	3	4	5	Avg Rank
End-users	4%	18%	7%	41%	30%	3.74
IT security function (CISO)	18%	20%	50%	8%	4%	2.59
IT leader (CIO)	14%	36%	23%	17%	10%	2.72
Human Resources	51%	14%	6%	8%	21%	2.33
Legal	12%	12%	13%	28%	36%	3.63

Japan	1	2	3	4	5	Avg Rank
End-users	7%	13%	12%	27%	41%	3.81
IT security function (CISO)	12%	20%	52%	11%	5%	2.77
IT leader (CIO)	19%	38%	23%	12%	7%	2.51
Human Resources	4%	10%	6%	48%	33%	3.95
Legal	58%	19%	3%	5%	14%	2.00

Q2: **AVERAGE RANK** Who **should be** most responsible for ensuring end-users' use of Internet applications and content sharing do not increase security risk for the organization?

Q2: **AVERAGE RANK**	US	UK	AU	FR	JP	Avg
End-users	2.19	2.25	2.11	3.74	3.81	2.82
IT security function (CISO)	2.63	2.74	2.73	2.59	2.77	2.69
IT leader (CIO)	2.70	2.66	2.56	2.72	2.51	2.63
Human Resources	3.83	3.79	3.87	2.33	3.95	3.55
Legal	3.67	3.59	3.76	3.63	2.00	3.33

Q2: **RANK ORDER**	US	UK	AU	FR	JP	Avg
End-users	1	1	1	5	4	2.40
IT security function (CISO)	2	3	3	2	3	2.60
IT leader (CIO)	3	2	2	3	2	2.40
Human Resources	5	5	5	1	5	4.20
Legal	4	4	4	4	1	3.40

Q3: In your opinion, do Web 2.0 applications interfere with the security posture of your company?	US	UK	AU	FR	JP	Avg
No	10%	11%	11%	26%	7%	13%
Yes, moderate impact	10%	31%	31%	29%	11%	22%
Yes, significant impact	34%	23%	22%	34%	33%	29%
Yes, very significant impact	46%	35%	36%	11%	49%	35%
Total	100%	100%	100%	100%	100%	100%

Q4: What threats or problems do Web 2.0 applications cause when downloaded and used? Please select no more than three threats or problems.	US	UK	AU	FR	JP	Avg
Viruses	49%	51%	52%	56%	63%	54%
Malware	52%	52%	48%	48%	61%	52%
SQL injections	14%	15%	11%	9%	36%	17%
Botnets	13%	17%	19%	17%	49%	23%
Workplace inefficiencies	63%	62%	60%	52%	26%	53%
Data loss	49%	51%	53%	49%	11%	43%
Bandwidth performance	10%	22%	19%	46%	16%	23%

Q5: Where on your list of security priorities does protecting your company against risks associated with Web 2.0 applications fall?	US	UK	AU	FR	JP	Avg
Very high priority	32%	10%	11%	13%	37%	21%
High priority	33%	33%	32%	12%	31%	28%
Medium priority	13%	35%	36%	12%	11%	21%
Low priority	11%	9%	12%	42%	9%	17%
Not a priority	12%	12%	9%	21%	12%	13%
Total	100%	100%	100%	100%	100%	100%

Q6: When do you plan to address the security of Web 2.0 applications?	US	UK	AU	FR	JP	Avg
Now	36%	11%	13%	15%	31%	21%
1-2 years	16%	25%	26%	26%	13%	21%
2-5 years	29%	43%	38%	40%	27%	35%
5-7 years	2%	2%	4%	3%	3%	3%
More than 7 years	2%	3%	3%	2%	3%	3%
Already addressed	10%	11%	12%	10%	21%	13%
Never	6%	6%	4%	4%	3%	5%
Total	100%	100%	100%	100%	100%	100%

D1. What organizational level best describes your current position?	US	UK	AU	FR	JP	Avg
Senior Executive	0%	2%	1%	1%	1%	1%
Vice President	1%	0%	2%	0%	0%	1%
Director	15%	7%	10%	6%	8%	9%
Manager	19%	21%	15%	20%	21%	19%
Supervisor	17%	24%	28%	24%	24%	24%
Technician	28%	30%	32%	30%	32%	30%
Staff	13%	6%	0%	7%	1%	6%
Contractor	5%	5%	8%	12%	12%	8%
Other	3%	4%	4%	0%	2%	2%
Total	100%	100%	100%	100%	100%	100%

D2. Is this a full time position?	US	UK	AU	FR	JP	Avg
Yes	90%	94%	100%	89%	100%	95%
No	10%	6%	0%	11%	0%	5%
Total	100%	100%	100%	100%	100%	100%

D3. Check the **Primary Person** you or your supervisor reports to within the organization.	US	UK	AU	FR	JP	Avg
Chief information officer	53%	60%	61%	55%	70%	60%
Chief technology officer	10%	8%	8%	9%	10%	9%
Chief information security officer	16%	9%	11%	12%	8%	11%
Chief security offer	6%	5%	3%	4%	5%	5%
Chief financial officer	3%	4%	3%	6%	0%	3%
Compliance Officer	2%	3%	4%	0%	0%	2%
Human Resources VP	1%	0%	4%	5%	0%	2%
Chief risk officer	6%	5%	5%	3%	3%	4%
Other	3%	6%	1%	6%	4%	4%
Total	100%	100%	100%	100%	100%	100%

D4. Total years of IT or security experience	US	UK	AU	FR	JP	Avg
Mean	10.31	9.56	8.84	9.92	8.50	9.42
Median	9.50	9.00	8.50	10.25	8.50	9.50

D5. Gender	US	UK	AU	FR	JP	Avg
Female	32%	29%	35%	27%	19%	28%
Male	68%	71%	65%	73%	81%	72%
Total	100%	100%	100%	100%	100%	100%

D6. What industry best describes your organization's industry focus?	US	UK	AU	FR	JP	Avg
Airlines	2%	1%	2%	1%	1%	2%
Automotive	2%	1%	0%	1%	3%	1%
Brokerage & Investments	2%	1%	6%	2%	7%	4%
Communications	2%	3%	6%	3%	7%	4%
Chemicals	7%	3%	5%	6%	4%	5%
Credit Cards	3%	5%	2%	2%	2%	3%
Defense	2%	8%	4%	2%	7%	4%
Education	5%	5%	6%	5%	5%	5%
Energy	5%	4%	5%	2%	4%	4%
Entertainment and Media	7%	2%	7%	2%	5%	5%
Federal Government	6%	6%	6%	0%	4%	4%
Food Service	0%	6%	3%	0%	4%	3%
Healthcare	4%	5%	0%	6%	1%	3%
Hospitality	3%	1%	7%	3%	4%	4%
Manufacturing	5%	7%	3%	7%	5%	5%
Insurance	7%	5%	3%	5%	2%	5%
Internet & ISPs	0%	1%	0%	1%	2%	1%
State or Local Government	3%	4%	3%	3%	1%	3%

Pharmaceuticals	5%	5%	1%	8%	2%	4%
Professional Services	4%	3%	1%	4%	5%	3%
Research	2%	0%	4%	0%	1%	1%
Retailing	7%	7%	7%	12%	9%	8%
Retail Banking	8%	9%	4%	9%	6%	7%
Services	2%	2%	6%	8%	0%	3%
Technology & Software	5%	5%	7%	6%	7%	6%
Transportation	1%	2%	2%	1%	2%	2%
Total	100%	100%	100%	100%	100%	100%

D7. Where are your employees located? (check all that apply):	US	UK	AU	FR	JP	Avg
United States	100%	71%	55%	50%	86%	72%
Canada	87%	68%	47%	46%	47%	59%
Europe	81%	71%	50%	50%	44%	59%
Middle east	37%	42%	29%	41%	43%	38%
Asia-Pacific	61%	48%	100%	37%	100%	69%
Latin America	40%	29%	30%	28%	59%	37%
Total	100%	100%	100%	100%	100%	100%

D8. What is the worldwide headcount of your organization?	US	UK	AU	FR	JP	Avg
Less than 500 people	11%	18%	21%	19%	16%	17%
500 to 1,000 people	13%	14%	22%	20%	15%	17%
1,001 to 5,000 people	26%	32%	28%	27%	23%	27%
5,001 to 25,000 people	27%	16%	23%	21%	25%	22%
25,001 to 75,000 people	13%	16%	4%	8%	14%	11%
More than 75,000 people	10%	4%	2%	5%	7%	6%
Total	100%	100%	100%	100%	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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 company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.