

Web 2.0 WorkTM

Independent Market
Research Report by



DYNAMIC MARKETS

Commissioned by

websense[®]

ESSENTIAL INFORMATION PROTECTION[™]

April 2009

Copyright notice

The copyright of this independent market research report remains with Dynamic Markets Limited, regardless of the medium this report may be stored in. The report may be reproduced, but only in its entirety; no abridgements or additions may be made without the specific written consent of Dynamic Markets Limited.

Published by

Dr Cherry Taylor (BSc, PhD)
Dynamic Markets Limited
PO Box 19
Abergavenny
NP7 8YF
UK
Tel: +44 870 7076767

Table of Contents

1. Executive Summary.....	1
2. Research Methodology.....	7
3. Key Findings	9
3.1. Web security confidence levels	9
3.2. Web security solutions in place	11
3.3. Access to Web 2.0 sites	13
3.4. Levels of awareness of Web 2.0 sites.....	15
3.5. Attitudes towards Web 2.0 sites and technology	17
3.6. Perception about the sources of Web security threats.....	18
3.7. Pressure from within to allow access to Web 2.0 sites	20
3.8. Pressure on IT security strategies	22
3.9. Users bypassing Web security policies	24
3.10. Consequences of an Internet security breach	25
Appendix A: Quantitative Questionnaire.....	27

1. Executive Summary

Global understanding - Web 2.0? [Section 3.4]

- When offered a list of Web 2.0 types of site, only 17% of global IT managers in large companies identified correctly that *all* of them would come under the banner of Web 2.0.
- In fact, the average number selected from a list of 10 categories is just 6 per IT manager.
- This demonstrates that while 87% were able to identify at least 1 as a Web 2.0 site, very few have a complete understanding of the extent to which this type of interactive technology is being used across the Internet today.
- Nevertheless, the three most commonly recognized categories of Web 2.0 are:
 1. Social networks used primarily for personal use, e.g. Facebook (65%)
 2. Social networks used primarily for business use, e.g. LinkedIn (64%)
 3. Web portals such as iGoogle (61%).
- But only approximately 1 in 2 IT managers consider sites like Wikis (53%) to be Web 2.0, and the same is true for sites enabling users to upload video (52%) or photographs (50%).
- And only 50% consider hosted software / cloud computing sites such as Salesforce.com to be of the Web 2.0 generation.
- With just under 1 in 2 IT managers selecting them, the least awareness of Web 2.0 sites surrounds those offering email services, like Hotmail (47%), hosting services, like Yahoo! Geocities (46%) and, bottom of the list, auction sites (36%).
- Around the world, IT managers in the APAC region consider more of these types of site to fall under the Web 2.0 banner, compared to EMEA and North America.
- Worse still, 14% of IT managers from large companies around the world do not consider *any* of these types of site to come under the banner of Web 2.0.
- Furthermore, 62% of IT managers were adamant that at least 1 of these sites did not qualify as a Web 2.0 site.
- However, more IT managers in North America (67%) consider at least 1 of these types of site not to belong to the Web 2.0 generation, compared to the APAC (60%) and EMEA (59%) regions.
- And among the whole sample, 37% admitted they were uncertain about at least 1 category and whether it qualifies as Web 2.0: indeed, uncertainty levels are high for all of these and range from 16% for personal social network sites, to 25% for hosted software / cloud computing sites.
- Also more IT managers in the EMEA (41%) and APAC (38%) regions are uncertain about at least 1 of these elements, compared to North America (31%).

Pressure to allow access?

Allowing access? [Section 3.3]

- Whether through ignorance or not, 95% of organizations allow access to Web 2.0 sites: indeed, on average, organizations allow access to 6 categories of Web 2.0 sites.
- In contrast, only 5% of organizations do not allow their users access to any Web 2.0 sites, 74% block access to at least 1, and organizations block on average 5 types of site.
- The types of Web 2.0 sites most commonly allowed access to by these large organizations are sites that provide email services, such as Hotmail, Yahoo, Gmail etc (77%).
- This is followed very closely by access to Web portals, such as iGoogle (74%), and also to Wikis (71%).
- 64% of IT managers permit access to social network sites primarily used for business, but a significant 1 in 2 organizations (49%) allow access to social network sites primarily used for personal use.
- Indeed, roughly 1 in 2 organizations allow users access to auction sites (52%), hosting services such as Yahoo! Geocities (50%) and hosted software / cloud computing sites such as Salesforce.com (48%).
- Furthermore, 56% of organizations allow users access to sites enabling users to upload photographs and 45% allow access to those that enable users to upload video material.
- Around the world, IT managers in North America allow access to more of these types of Web 2.0 sites, compared to the APAC and EMEA regions.
- But overall, the Top 3 most commonly denied Web 2.0 site categories for the whole sample are:
 1. Social networking sites used primarily for personal use (e.g. Facebook) (48%)
 2. Social networking sites primarily used for business (e.g. LinkedIn) (30%)
 3. Email services such as Hotmail, Yahoo, Gmail etc (22%).
- Yet, rather worryingly, 27% of global IT managers in large organizations are not sure about the access status of some Web 2.0 sites: and ignorance is especially high around the use of hosted software / cloud computing sites such as Salesforce.com (16%) and hosting services, such as Yahoo! Geocities (10%).
- Organizations in North America allow access to a wider variety of Web 2.0 sites; but the APAC region stands out as allowing access to fewer Web 2.0 sites and denying access to more of them.

Feeling the pressure? [Sections 3.5, 3.7 & 3.8]

- On the one hand, 62% of IT managers think Web 2.0 is necessary to their business, whereas fewer (24%) do not.
- But the users in these large organizations seem quite definite about wanting access to Web 2.0 sites; indeed, 86% of IT managers feel pressurized to allow access to Web 2.0 sites from within their organization, and for many of these, pressure is coming from more than 1 area of the business.

- Marketing (34%) and sales (32%) are guilty in equal measures when it comes to applying the pressure; and C-level / director level staff themselves are applying pressure in 30% of organizations, whereas fewer finance (16%) and HR (21%) departments are doing this.
- But while 32% of IT managers say they feel pressure from users wanting to use Web 2.0 sites for business, almost as many (30%) feel pressure from users wanting personal time on Web 2.0 sites.
- Users in large companies in APAC are fighting back against a relative lack of access with more of them applying pressure on their IT managers to allow access to Web 2.0 sites.
- In contrast, there is less pressure coming from users in large companies in EMEA.
- But users want protection *and* access and this pressure is followed through into IT security strategies, with users in 66% of organizations wanting safe access:
 - 45% of IT managers are under pressure to include something about how to empower and protect Internet users without being overly restrictive.
 - 41% are under pressure to include something about how to enable access to Web 2.0 sites without security worries.
 - 41% are under pressure to include a means of keeping up with the ever-changing threat landscape in real time.
- But, in a similar vein, 62% of IT managers are under pressure to include an area covering the protection from leakage of company-confidential information and 55% are expected to include protection from inbound Web and email security threats.
- But fewer than 1 in 2 are under pressure to build in regulatory compliance measures (49%), protection of users' personal data (45%), or to demonstrate an understanding and identification of where confidential data resides for the company (43%).
- The research shows that IT managers in North America are under pressure to include more of these areas within their IT security strategies, compared to their counterparts in APAC and EMEA; notably in areas such as protection from leakage of company-confidential information, understanding and identification of where confidential data resides for the company and to build regulatory compliance measures into their IT security strategy.

Obedient users? [Section 3.9]

- The research suggests that 94% of organizations have Web security policies in place in an attempt to restrict users' access to certain areas of the Internet.
- Yet 47% of IT managers say the users in their organization try and bypass their Web security policies.
- The worst users in this respect reside in APAC and North America – whereas rebellion of this nature is less common in EMEA.
- In contrast, 33% say their users do not behave in this way and another 14% are not sure if users do or not.

Real protection against the Internet?

Source of the problem? [Section 3.6]

- Indeed, when it comes to protection against Internet security threats, 58% of global IT managers think one area of the Internet holds more of a security threat than another.
- Specifically, 15% think the ‘dynamic’ Web (or the Top 100 most popular sites) holds the most Web security threats, but as many (15%) think the biggest threat comes from the ‘known’ Web (or the next 1 million sites); but more (28%) think the ‘unknown’ Web (or the next 100 million sites) holds the most threats.
- In contrast, 38% of IT managers feel that there is no particular area of the Internet that is safe and that threats are everywhere in equal measure.
- Most North American IT managers responded this way (43%), whereas fewer IT managers in APAC (32%) felt that all areas of the Internet are equally dangerous.
- Threats can occur everywhere on the Internet - however, research from Websense Security Labs¹ shows that the top 100 most popular sites on the Web are a fast-growing target for attackers and sites allowing user-generated content comprise the majority of the top 50 most active distributors of malicious content on the Web.

False confidence? [Sections 3.1 & 3.2]

- But perhaps users have nothing to fear, as 80% of IT managers are confident about their organization’s Web security: a very confident 22% think their company is 100% protected, and another 58% are confident that they have as much protection as they need, but admit that some threats will always get in.
- The most confident IT managers are to be found in EMEA, whereas fewer come from North America.
- In contrast, 11% of global IT managers are worried and frustrated that Web security is not being addressed internally through lack of interest and / or budget and / or resources – especially in North America (14%).
- Similarly, 7% are worried and know that their organization is overdue at addressing Web security.
- So is this confidence justified? Indeed, the research shows that 94% of organizations have some form of additional security solution in place, in addition to any firewall and antivirus solutions they may have, but only 9% have solutions in place to cover *all* threat areas.
- That said, the most common additional solution in place is URL filtering (61%), but this means 39% do not have this area covered.
- 58% have a solution to block phishing sites, and as many claim to have real-time detection of malware (58%).

¹ Source: “State of Internet Security, Q3 – Q4 2008” by Websense Security Labs

- 55% say they have a solution that protects company-confidential data from being uploaded on to the Web – but this means 45% of organizations are vulnerable in this respect.
- 54% claim to have a solution that enables real-time prevention of malware entering the network – meaning 46% do not.
- But fewer than 1 in 2 companies are able to detect malicious code on trusted Web sites (48%), or stop spyware from sending out information to external sources (47%), or stop safe Web sites from routing browsers to unknown sites (41%), and almost as many (40%) are able to block instant messaging attachments.
- Alarmingly for users, only roughly a third of IT managers claim to have solutions in place that can provide real-time analysis of Web site content (36%) or real-time Web content classification (32%) – a threat that is especially real on Web 2.0 sites.
- Around the world, IT managers in the APAC region have more of these vulnerable areas covered, whereas companies in EMEA and North America have the least protection in place.

Consequences? [Section 3.10]

- If an Internet security breach were to occur that resulted in data loss or had a significant, negative effect on the business, understandably 95% of IT managers would have concerns.
- Indeed, IT managers in North America and the APAC regions would have relatively more concerns, whereas those in EMEA would have fewer.
- From an internal perspective, 29% of IT managers would be concerned about the Executive Board being notified, and another 20% would worry about a full post-mortem taking place.
- And 40% would worry about the IT department being held accountable, but 1 in 5 (21%) would actually be worried about losing their jobs – and this fear is relatively more common in APAC (24%) and North America (25%).
- In terms of external perception, more (54%) would be worried about the inevitable loss of faith from customers.
- But fewer than 1 in 2 would be concerned about public disclosure of the data breach (46%), financial penalties from regulatory bodies (36%), the negative media attention that might follow (44%), and the impact on the business from shareholders / investors (39%).
- But fewer than 1 in 2 (45%) IT managers would be concerned about urgently finding a solution for future protection.

2. Research Methodology

2.1 Overview:

This report was commissioned by Websense and details quantitative research with IT managers in large companies around the world.

2.2 Quantitative Research:

A sample of 1300 interviews was collected with IT managers in 10 countries: namely Australia, Canada, China, France, Germany, Hong Kong, India, Italy, the UK and the US. 100 interviews were collected in all countries, except the US where 400 were collected.

Respondents confirmed prior to interview that their organization has 250 or more PC users, thus all of them qualify as large companies by European definitions. They also confirmed their level of seniority: 32% operate at CIO / director level and 68% are at manager level. None of the sample are clerical or admin-level IT staff. Top-level IT staff dominate the samples of China (51%) and Italy (67%), whereas this level of management makes up a smaller proportion of the Australian (12%) and Indian (18%) samples.

Table 2.1: Level of seniority among country samples:

Country	CIO / IT director level	IT manager level
Australia	12%	88%
Canada	23%	77%
China	51%	49%
France	38%	62%
Germany	32%	68%
Hong Kong	28%	72%
India	18%	82%
Italy	67%	33%
The UK	30%	70%
The US	30%	70%

2.3 Comparative Analysis:

In this report, the findings of the survey have been analyzed and compared systematically according to territory. Table 2.2 shows the margin of error at a 95% confidence level and Table 2.3 shows the sub-sample sizes. These tables can be used to determine whether an observed difference between two sub-samples (e.g. the EMEA versus North America) is a *real* difference or not; in other words, to see if the difference is statistically significant.

This means that for an observed percentage of 5% on a sub-sample of 400 respondents, the *real* percentage could be +/-2.2%, so the *real* percentage could be anywhere between 2.8% and 7.2%. This means that if the survey were repeated under exactly the same conditions, there is a 95% chance of getting a number anywhere between 2.8% and 7.2%. It follows that if 2% of employees in EMEA selected a particular answer, compared to 8% of

employees in the APAC territory, from a statistical point of view, the observed difference is NOT statistically valid at a 95% confidence level. Therefore, where any differences exist that are significant at a 95% confidence level, and are relevant to the overall findings, they are described accordingly in this report.

Table 2.2: Margin of error at a 95% confidence level:

Sample size	50	100	200	300	400	500	1000
5% or 95%	±6.2	±4.4	±3.1	±2.5	±2.2	±1.9	±1.4
10% or 90%	±8.5	±6.0	±4.2	±3.5	±3.0	±2.7	±1.9
25% or 75%	±12.5	±8.7	±6.1	±5.0	±4.3	±3.9	±2.7
50%	±14.1	±10	±7.1	±5.8	±5.0	±4.5	±3.2

Table 2.3: Sub-sample sizes (n):

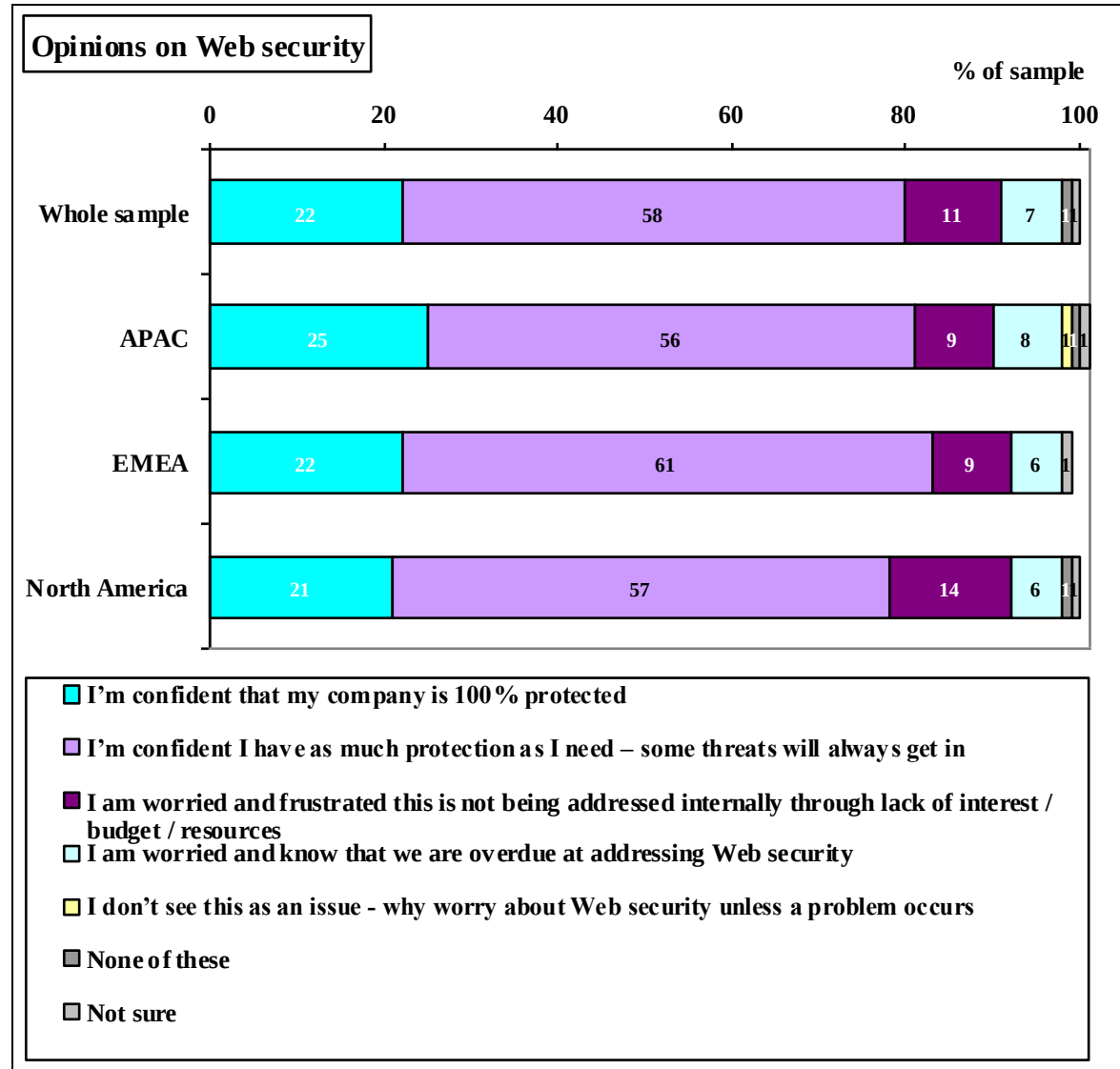
Territory	n=
APAC	400
EMEA	400
North America	500

The interviews were conducted using an online research panel between 6th and 18th February 2009. Before and during the interviews, respondents were not aware that Websense had commissioned the research.

Throughout this report, where any numbers do not add up to 100%, it is either because respondents were allowed to select more than one tick-box option in the question, or because of minor rounding errors, which should be ignored.

3. Key Findings

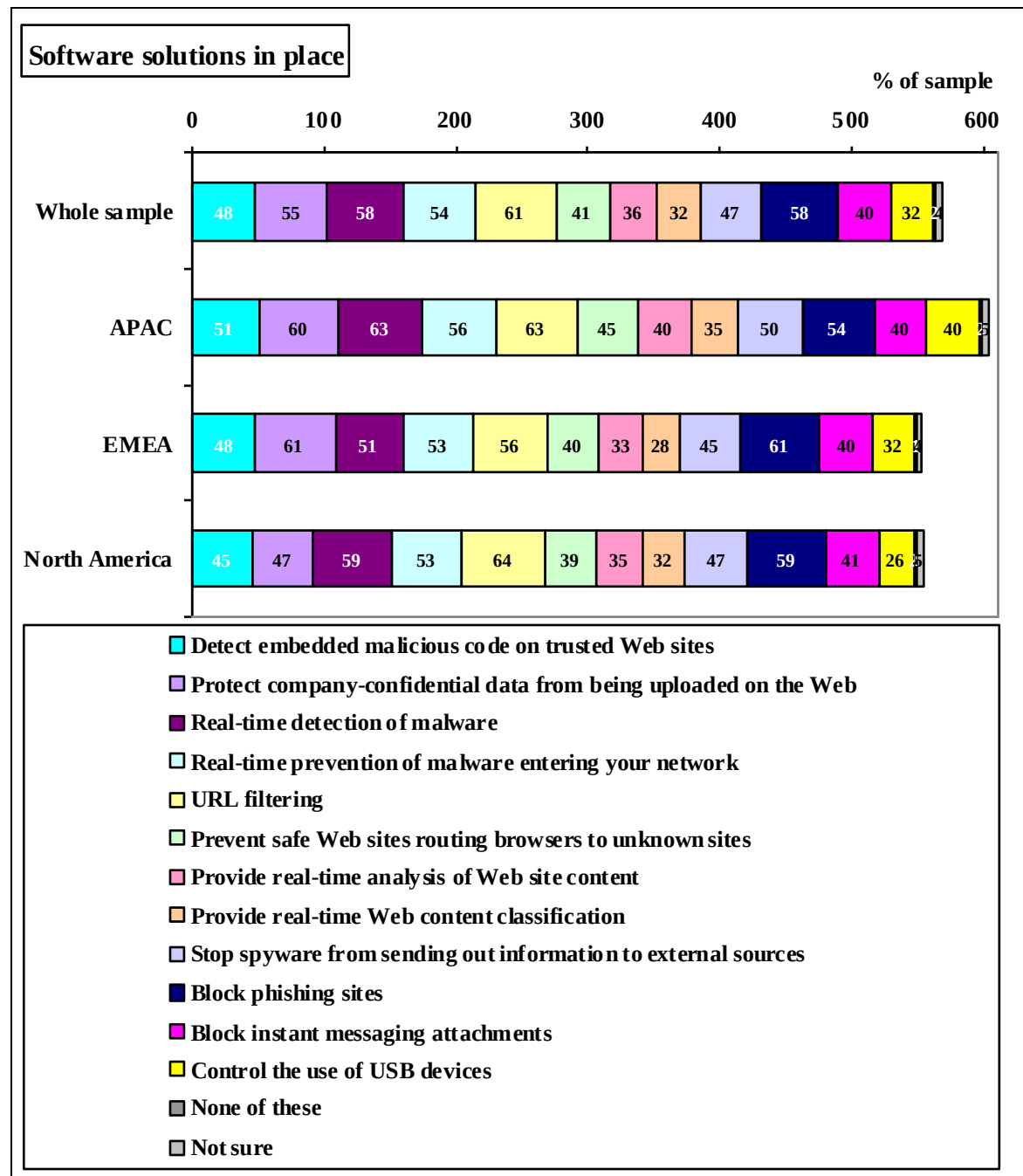
3.1. Which of the following statements represents how you feel about your company's Web security?



- Collectively, 80% of IT managers around the world are confident about their organization's Web security.
- In more detail, a very confident 22% think their company is 100% protected.
- Another 58% are confident that they have as much protection as they need, but they admit that some threats will always get in.
- In contrast, 11% are worried and frustrated that Web security is not being addressed internally through lack of interest and / or budget and / or resources.
- 7% are worried and know that their organization is overdue at addressing Web security.

- Fewer than 1% of the sample admit they do not see Web security as an issue, and take the approach of why worry about Web security unless a problem occurs.
- 1% say none of these statements sum up how they feel about their organization's Web security and another 1% are not sure how they feel in this respect.
- Around the world, more IT managers in the EMEA region (83%) are confident in their organizations' Web security, compared to North America (77%).
- In detail, more IT managers in North America (14%) are worried and frustrated that Web security is not being addressed internally through lack of interest and / or budget and / or resources, compared to the APAC and EMEA regions (both 9%).

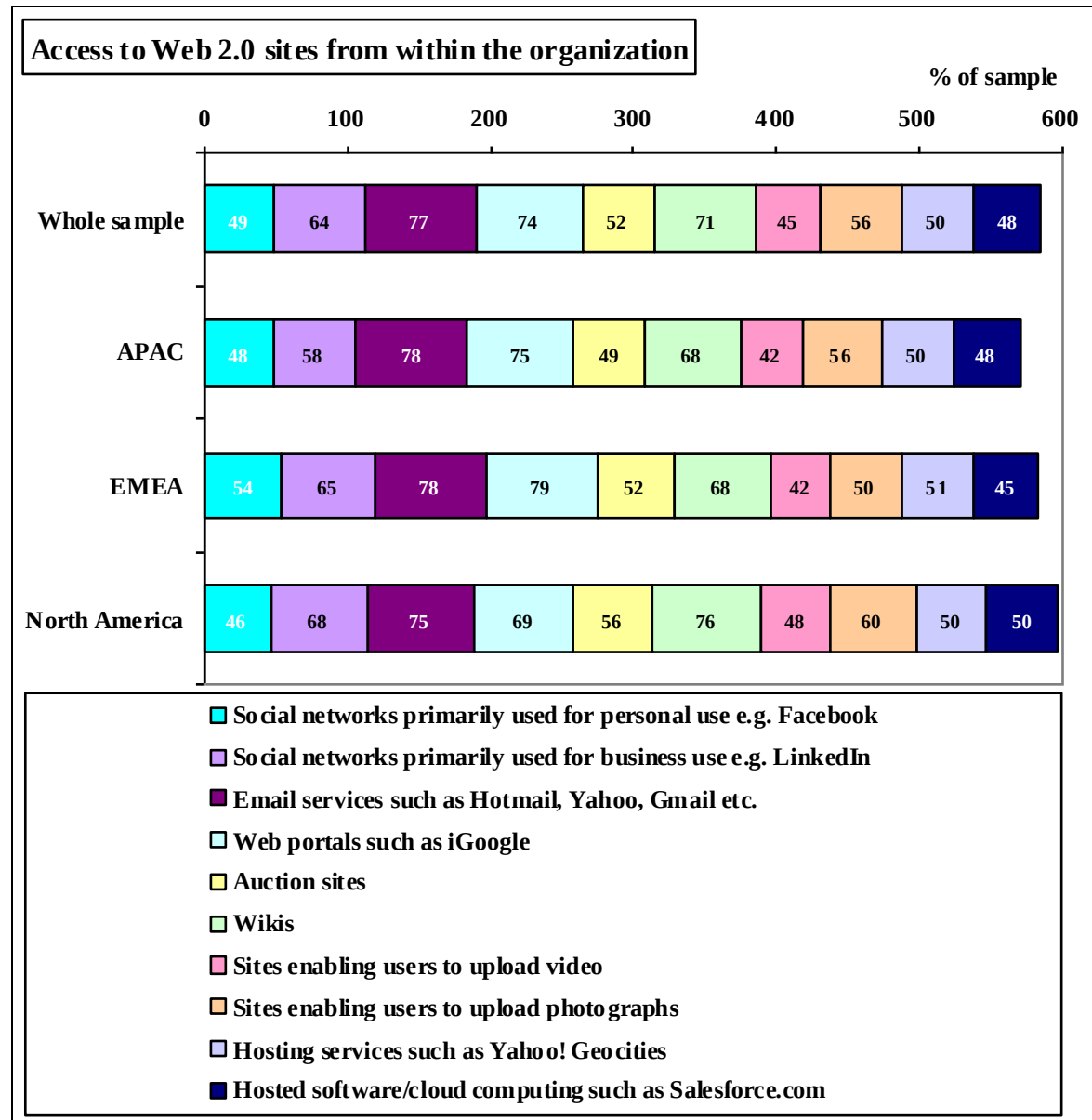
3.2. In addition to any firewall and antivirus solutions your organization has in place, does it have other specific solutions to do any of the following?



- Collectively, 94% of organizations around the world have at least 1 of these additional security solutions in place, in addition to any firewall and antivirus solutions they may have.
- In contrast, only 9% have solutions in place to cover *all* of these areas [not shown].
- The most common additional solution in place is URL filtering (61%), but this means that 39% do not have this area covered.

- 58% have a solution to block phishing sites, and as many claim to have real-time detection of malware (58%).
- 55% say they have a solution that protects company-confidential data from being uploaded on the Web – but this means 45% of organizations are vulnerable in this respect.
- 54% claim to have a solution that enables real-time prevention of malware entering the network – meaning 46% do not.
- But fewer than 1 in 2 companies are able to detect malicious code on trusted Web sites (48%), or stop spyware from sending out information to external sources (47%), or stop safe Web sites from routing browsers to unknown sites (41%) and almost as many (40%) are able to block instant messaging attachments.
- Only roughly a third claim to have solutions in place that can provide real-time analysis of Web site content (36%) or real-time Web content classification (32%).
- Despite their abundant use, only 32% are able to control the use of USB devices, meaning 68% cannot.
- In contrast, 2% of IT managers admit they do not have solutions in place to cover any of these Web security risks, and another 4% are unsure which are in place and which are not covered.
- Around the world, IT managers in the APAC region claim to have solutions in place that cover more of these Web security threat areas, compared to the EMEA and North America regions (i.e. length of bars in above chart).
- Indeed, more IT managers in the APAC region (11%) have solutions in place to cover *all* of these areas, compared to North America (7%) [not shown].
- In detail, more IT managers in the APAC (60%) and EMEA (61%) regions protect company-confidential data from being uploaded on the web, compared to North America (47%).
- But, more IT managers in the APAC (63%) and the North America (59%) regions claim to have real-time detection of malware, compared to the EMEA region (51%).
- And, more IT managers in the APAC (63%) and the North America (64%) regions have URL filtering, compared to the EMEA region (56%).
- Whereas, more IT managers in the APAC region (45%) stop safe Web sites from routing browsers to unknown sites, compared to North America (39%).
- Also, more IT managers in the APAC region (40%) have solutions in place that can provide real-time analysis of Web site content, compared to the EMEA region (33%).
- Finally, more IT managers in the APAC (40%) and EMEA (32%) regions are able to control the use of USB devices, compared to North America (26%).

3.3. Do you allow access to any of the following within your organization?

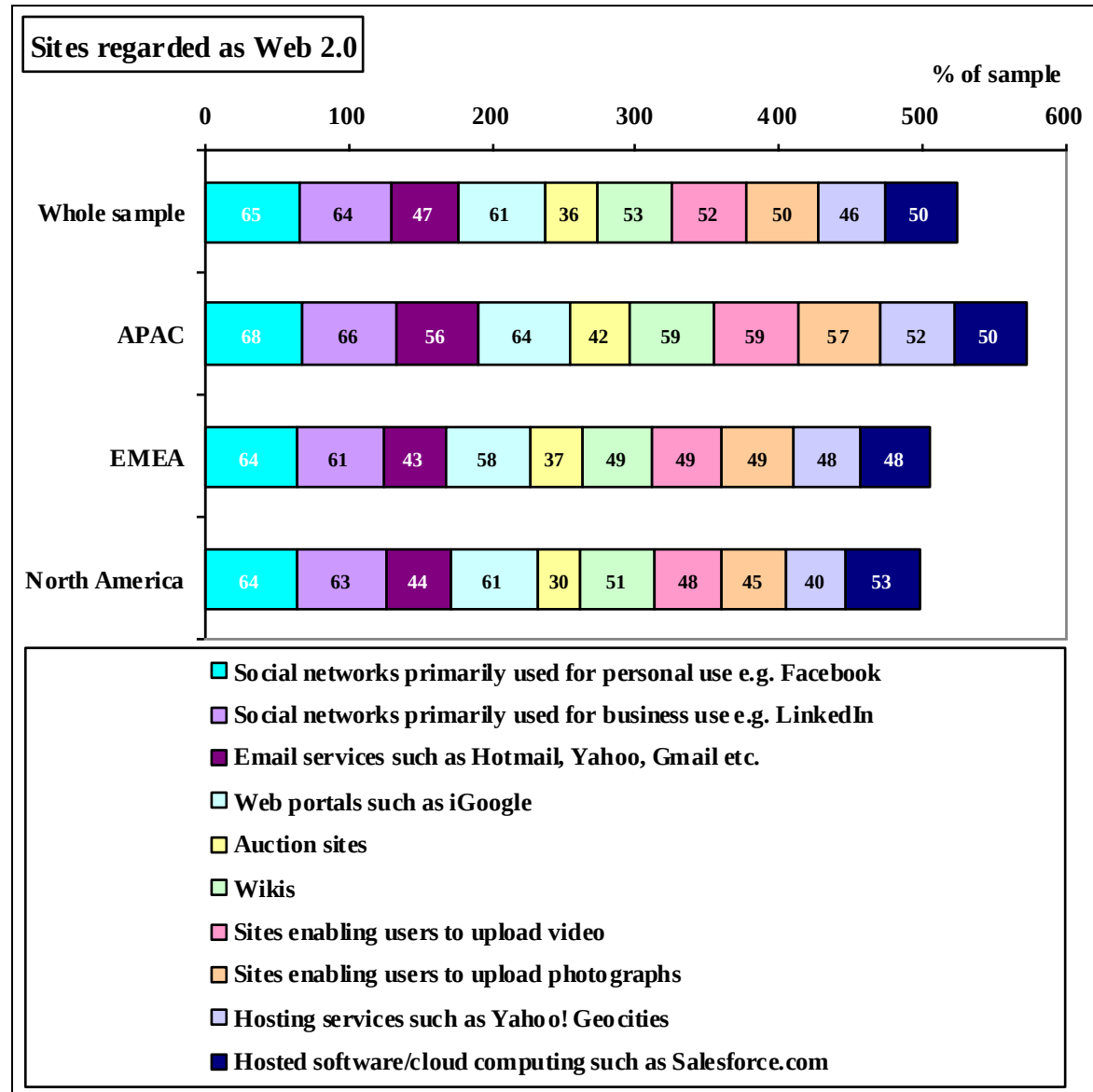


- Collectively, 95% of IT managers around the world allow access to at least 1 of these Web 2.0 sites [not shown].
- Indeed, on average, organizations allow access to 6 of these sites [not shown].
- The type of Web 2.0 sites most commonly allowed access to by these large organizations are sites that provide email services, such as Hotmail, Yahoo, Gmail etc (77%).
- This is followed very closely by access to Web portals, such as iGoogle (74%), and also to Wikis (71%).
- 64% of IT managers say the organization allows access to social network sites primarily used for business (e.g. LinkedIn), but a significant 1 in 2 organizations

(49%) allow access to social network sites primarily used for personal use (e.g. Facebook).

- Indeed, roughly 1 in 2 organizations allow users access to auction sites (52%), hosting services such as Yahoo! Geocities (50%) and hosted software / cloud computing sites such as Salesforce.com (48%).
- 56% of organizations allow users access to sites enabling users to upload photographs and 45% allow users to access those that enable users to upload video material.
- Around the world, IT managers in North America allow access to more of these types of Web 2.0 sites, compared to the APAC and EMEA regions (i.e. length of bars in above chart).
- But in detail, more IT managers in the EMEA region (54%) allow access to social network sites primarily used for personal use, compared to North America (46%).
- And, more IT managers in the EMEA (65%) and North America (68%) regions allow access to social network sites primarily used for business (e.g. LinkedIn), compared to the APAC region (58%).
- Also, more IT managers in the APAC (75%) and EMEA (79%) regions allow access to Web portals, such as iGoogle, compared to North America (69%).
- But, more IT managers in the North America region (56%) allow users access to auction sites, compared to the APAC region (49%).
- In addition, more IT managers in North America (76%) allow users access to Wikis, compared to the APAC and EMEA regions (both 68%).
- And, more IT managers in North America (60%) allow users access to sites enabling users to upload photographs, compared to the EMEA region (50%).
- In contrast, only 5% of organizations from all territories do not allow their users access to any of these Web 2.0 sites, and 74% block access to at least 1 [not shown].
- The Top 3 most commonly denied Web 2.0 sites are [not shown]:
 1. Social networking sites used primarily for personal use (e.g. Facebook) (48%)
 2. Social networking sites primarily used for business (30%)
 3. Email services such as Hotmail, Yahoo, Gmail etc (22%).
- On average, organizations block 5 such sites [not shown].
- Around the world, more IT managers in the APAC region (78%) deny access to at least 1 of these Web 2.0 sites, compared to the EMEA (72%) and North America (71%) regions [not shown].
- But 27% of all IT managers are not sure about the access status of at least 1 of these Web 2.0 sites – especially in the APAC (29%) and EMEA (30%) regions, compared to North America (23%) [not shown].
- And ignorance is especially high around the use of hosted software / cloud computing sites such as Salesforce.com (16%) and hosting services, such as Yahoo! Geocities (10%) [not shown].

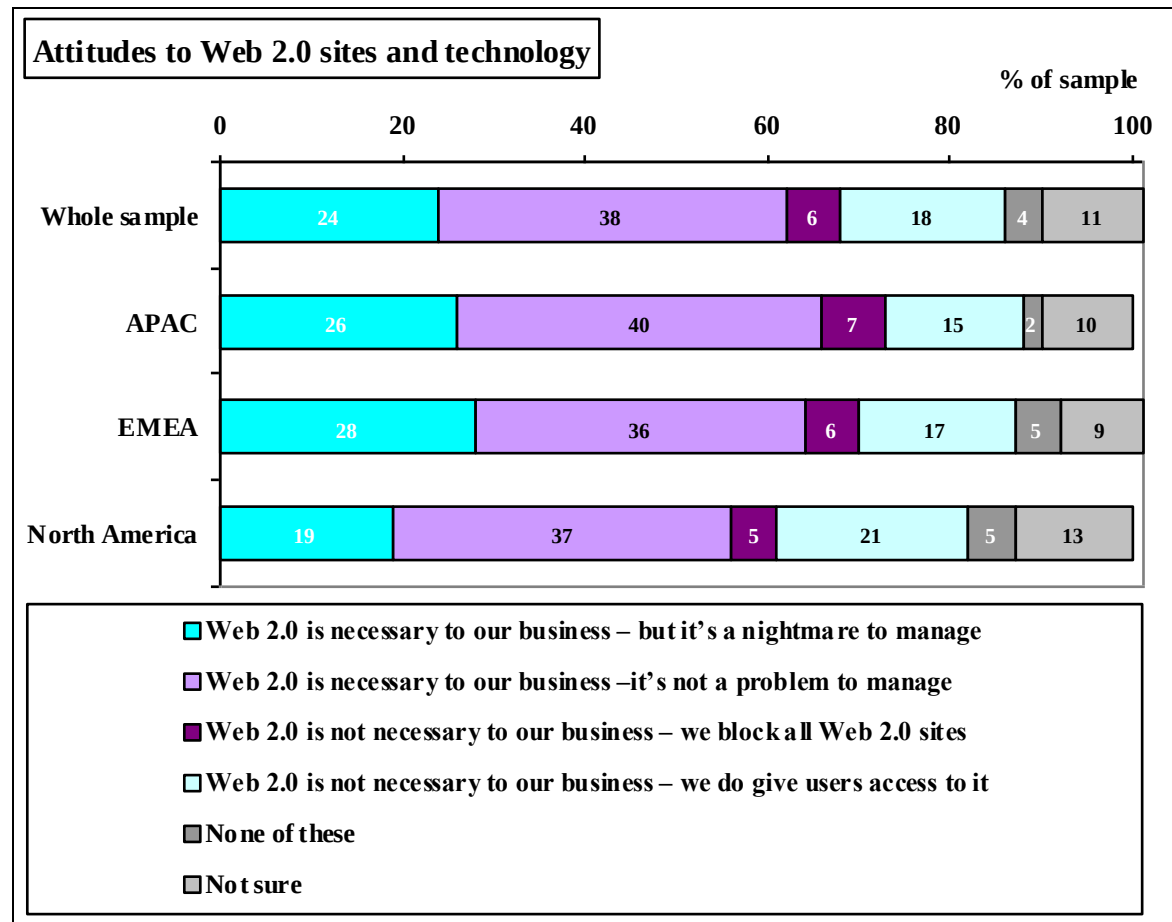
3.4. Which of the following elements would you consider to be Web 2.0?



- Collectively, just 86% of IT managers in the sample consider at least 1 of these types of Web site to be Web 2.0 [not shown].
- And only 17% identified correctly that they are *all* Web 2.0 types of site [not shown].
- In fact, the average number selected from this list of 10 Web 2.0 sites is just 6 [not shown].
- The three most commonly recognized elements as Web 2.0 sites are:
 1. Social networks used primarily for personal use, e.g. Facebook (65%)
 2. Social networks used primarily for business use, e.g. LinkedIn (64%)
 3. Web portals such as iGoogle (61%).
- But only approximately 1 in 2 IT managers consider sites like Wikis (53%) to be Web 2.0, and the same is true for sites enabling users to upload video (52%) or photographs (50%).

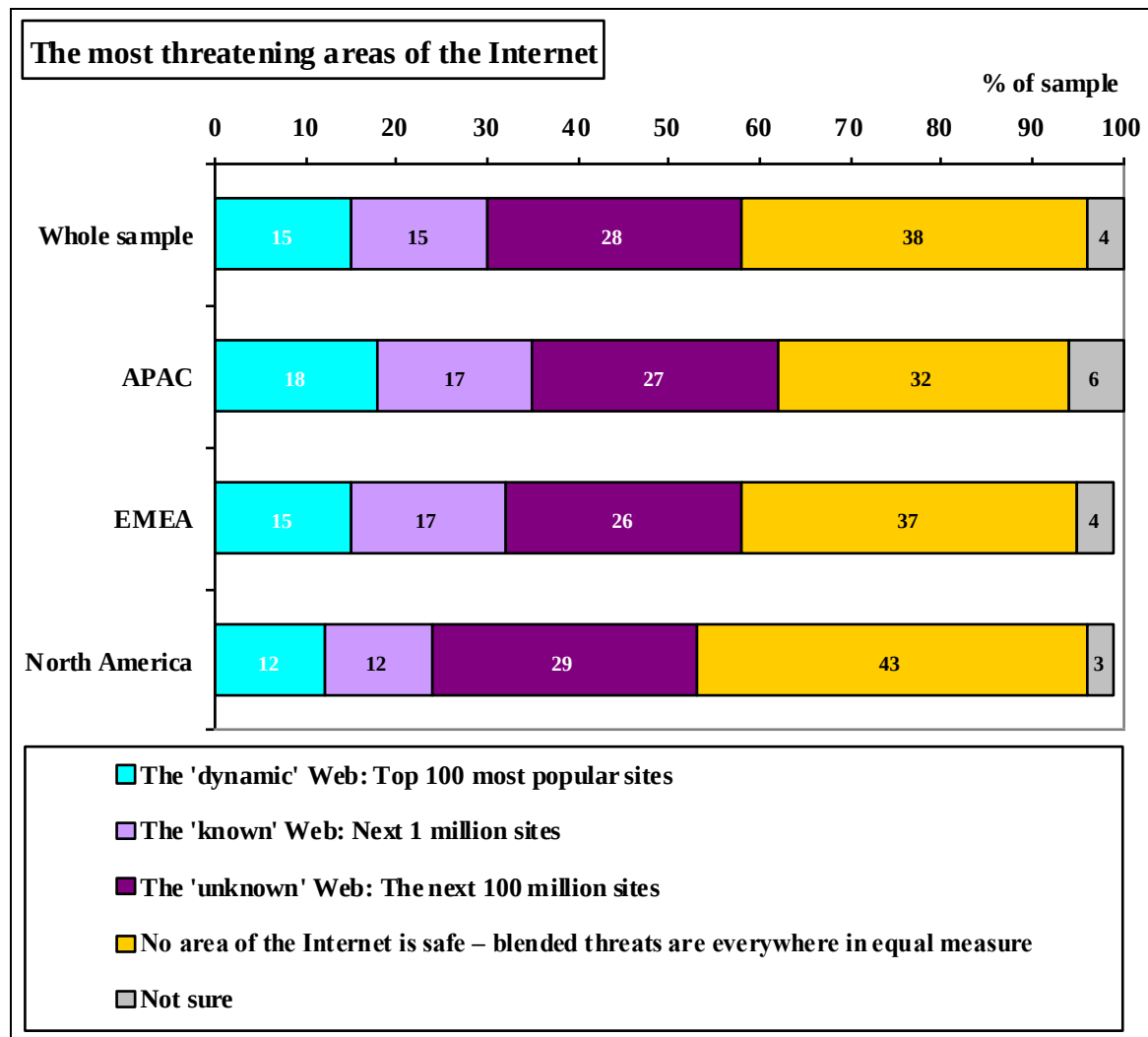
- And only 50% consider hosted software / cloud computing sites such as Salesforce.com to be of the Web 2.0 generation.
- With just under 1 in 2 IT managers selecting them, the least awareness of Web 2.0 sites surrounds those offering email services, like Hotmail (47%), hosting services, like Yahoo! Geocities (46%) and, bottom of the list, auction sites (36%).
- Around the world, IT managers in the APAC region consider more of these sites to fall under the Web 2.0 banner, compared to the EMEA and North America regions (i.e. length of bars in the above chart).
- Indeed, more IT managers in the APAC region (89%) consider at least 1 of these types of Web sites to be Web 2.0, compared to the EMEA region (84%) [not shown].
- And, more IT managers in the APAC region (20%) consider them *all* to be Web 2.0 sites, compared to North America (15%) [not shown].
- In more detail, more IT managers in the APAC region (56%) consider email services, like Hotmail, to be Web 2.0, compared to the EMEA (43%) and North America (44%) regions.
- Yet, more IT managers in the APAC (42%) and EMEA (37%) regions consider auction sites to be Web 2.0, compared to North America (30%).
- And, more IT managers in the APAC region (59%) consider Wikis to be a Web 2.0 site, compared to the EMEA (49%) and North America (51%) regions.
- Also, more IT managers in the APAC region (59%) consider sites enabling users to upload video to be Web 2.0 sites, compared to the EMEA (49%) and North America (48%) regions.
- In addition, more IT managers in the APAC region (57%) consider sites enabling users to upload photographs to be Web 2.0 sites, compared to the EMEA (49%) and North America (45%) regions.
- But, more IT managers in the APAC (52%) and EMEA (48%) regions consider hosting services, like Yahoo! Geocities to be Web 2.0 sites, compared to the North America region (40%).
- In contrast, 14% of all IT managers do not consider any of these types of site to come under the banner of Web 2.0 [not shown].
- And 62% said at least 1 of these sites did not qualify as a Web 2.0 site [not shown].
- And more IT managers in North America (67%) consider at least 1 of these types of site not to belong to the Web 2.0 generation, compared to the APAC (60%) and EMEA (59%) regions [not shown].
- But 37% of all IT managers were uncertain about at least 1 of these sites and whether they qualify as Web 2.0: indeed, uncertainty levels are high for all of these and range from 16% for personal social network sites, e.g. Facebook, to 25% for hosted software / cloud computing sites [not shown].
- And more IT managers in the EMEA (41%) and APAC (38%) regions were uncertain about at least 1 of these elements, compared to North America (31%) [not shown].

3.5. Which of the following best describes your attitude to Web 2.0 sites and technology?



- Collectively, 62% of IT managers from around the world think that Web 2.0 is necessary to their business.
- However, this breaks down into those that think it is necessary, but a nightmare to manage (24%), and those who think it is necessary and not a problem to manage (38%).
- In contrast, 24% do not think Web 2.0 is necessary to their business and then 6% block all Web 2.0 sites, whereas 18% give users access to them.
- This means 80% of organizations give their users access to what they consider to be Web 2.0 sites.
- 4% say none of these best describes their attitude towards Web 2.0 sites and technology, and another 11% are unsure which, if any, apply.
- Around the world, more IT managers in the APAC (66%) and EMEA (64%) regions think Web 2.0 sites are necessary to their business, compared to North America (56%).
- However, more IT managers in the APAC (26%) and EMEA (28%) regions think Web 2.0 is necessary, but a nightmare to manage, compared to North America (19%).
- But, more IT managers in North America (21%) think such sites are not necessary, but allow users access to them anyway, compared to the APAC region (15%).

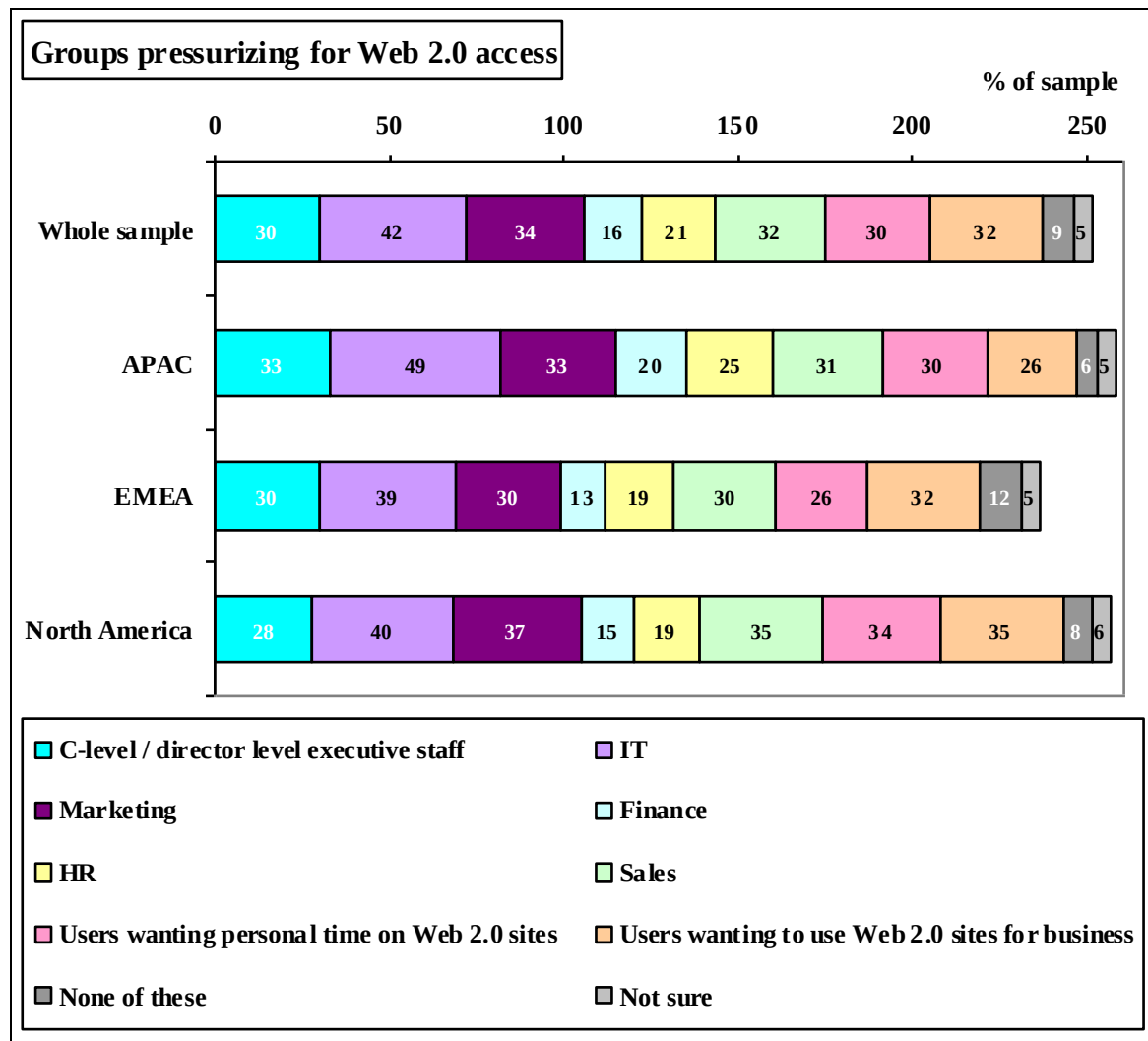
3.6. Which one of the following areas of the Internet do you feel holds the most Web security threats?



- 58% of IT managers think at least 1 area of the Internet holds more of a security threat than others.
- In detail, 15% think the 'dynamic' Web (or the Top 100 most popular sites) holds the most Web security threats.
- As many (15%) think the biggest threat comes from the 'known' Web (or the next 1 million sites).
- More (28%) think the 'unknown' Web (or the next 100 million sites) holds the most threats.
- But 38% of IT managers feel no area of the Internet is safe and that threats are everywhere in equal measure.
- Another 4% of IT managers are unsure where the greatest level of Web security threat comes from on the Internet.

- Around the world, more IT managers in the APAC region (62%) think at least 1 area of the Internet holds more of a security threat than others, compared to North America (53%).
- In more detail, more IT managers in the APAC region (18%) think the ‘dynamic’ Web (or the Top 100 most popular sites) holds the most Web security threats, compared to North America (12%).
- And, more IT managers in the APAC and EMEA (both 17%) regions think the biggest threat comes from the ‘known’ Web (or the next 1 million sites), compared to North America (12%).
- However, more IT managers in North America (43%) feel no area of the Internet is safe and that blended threats are everywhere in equal measure, compared to the APAC (32%) and EMEA (37%) regions.

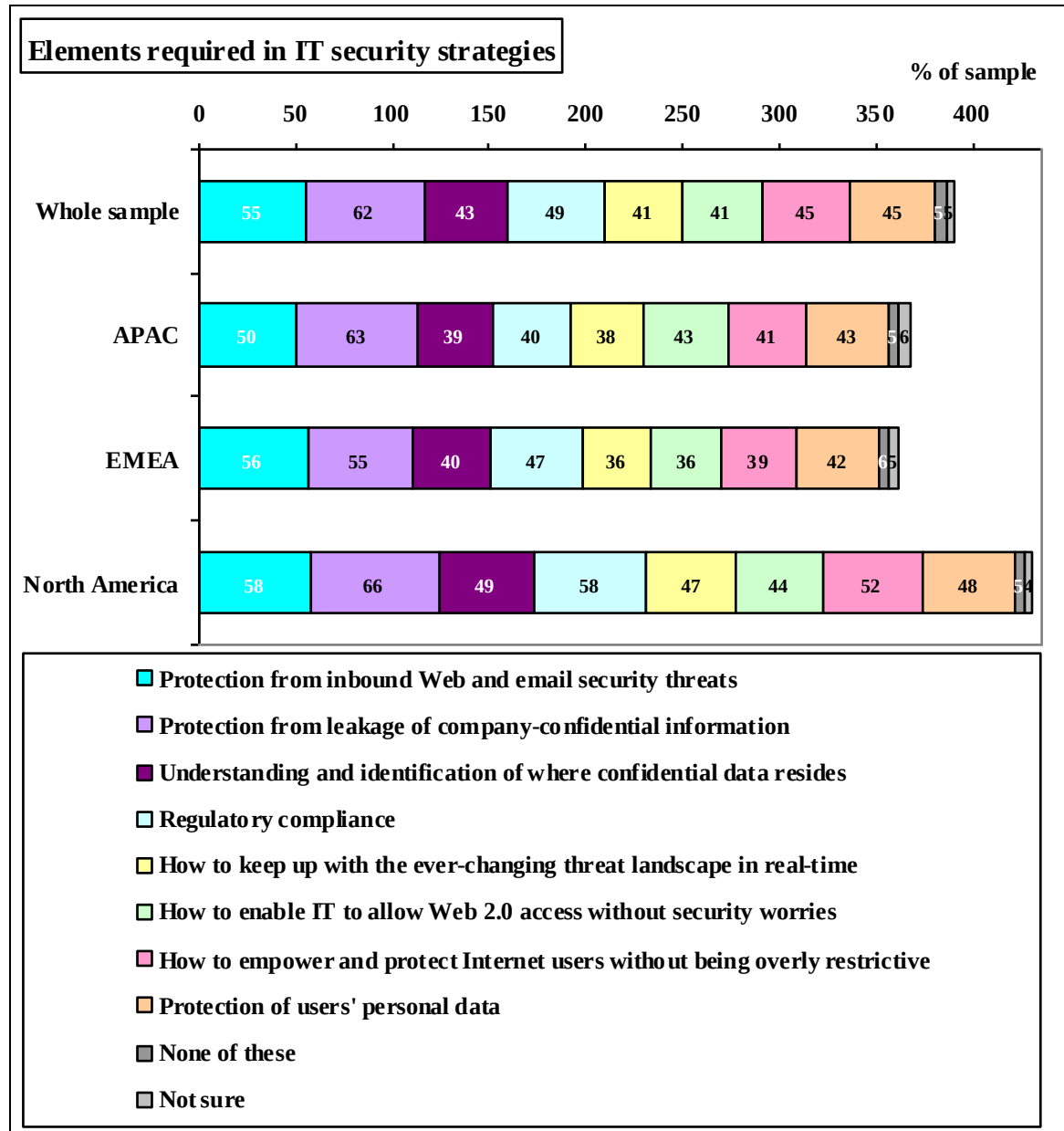
3.7. From which of the following groups within your organization do you feel pressure to allow access to Web 2.0 sites?



- Collectively, 86% of IT managers feel pressurized to allow access to Web 2.0 sites from at least 1 group of people from within their organization.
- Indeed, 57% feel such pressure from multiple groups, and 40% feel it from 3 or more areas of the business [not shown].
- In fact, the group most commonly putting pressure on IT managers to allow access is actually the IT department itself (42%).
- Marketing (34%) and sales (32%) are equally guilty of applying the pressure for access to Web 2.0 sites.
- C-level / director level staff themselves are applying pressure in 30% of organizations, whereas fewer finance (16%) and HR (21%) departments are doing this.
- While 32% of IT managers say they feel pressure from users wanting to use Web 2.0 sites for business, almost as many (30%) feel pressure from users wanting personal time on Web 2.0 sites.

- In contrast, 9% of IT managers say they do not feel any pressure from within the organization to allow access to Web 2.0 sites.
- Another 5% are unsure where such pressure, if any, comes from.
- Around the world, IT managers in the APAC and North America regions feel pressure from more of these groups to allow access to Web 2.0 sites, compared to those in the EMEA region (i.e. length of the bars in the above chart).
- In fact, more IT managers in the APAC region (89%) feel pressurized to allow access to Web 2.0 sites from at least 1 group from within their organization, compared to in the EMEA region (83%).
- In more detail, more IT managers in the APAC region (49%) feel pressurized by the IT department, compared to in the EMEA (39%) and North America (40%) regions.
- But, more IT managers in North America (37%) feel pressurized by marketing, compared to in the EMEA region (30%).
- Whereas, more IT managers in the APAC region (20%) feel pressurized by the finance department, compared to in the EMEA region (13%).
- And more IT managers in the APAC region (25%) feel pressurized by the HR department, compared to North America (19%).
- However, more IT managers in North America (34%) feel pressure from users wanting personal time on Web 2.0 sites, compared to in the EMEA region (26%).
- Yet, more IT managers in the North America region (35%) feel pressure from users wanting to use Web 2.0 sites for business, compared to the APAC region (26%).
- In contrast, more IT managers in the EMEA region (12%) say they do not feel any pressure from within the organization to allow access to Web 2.0 sites, compared to in the APAC region (6%).

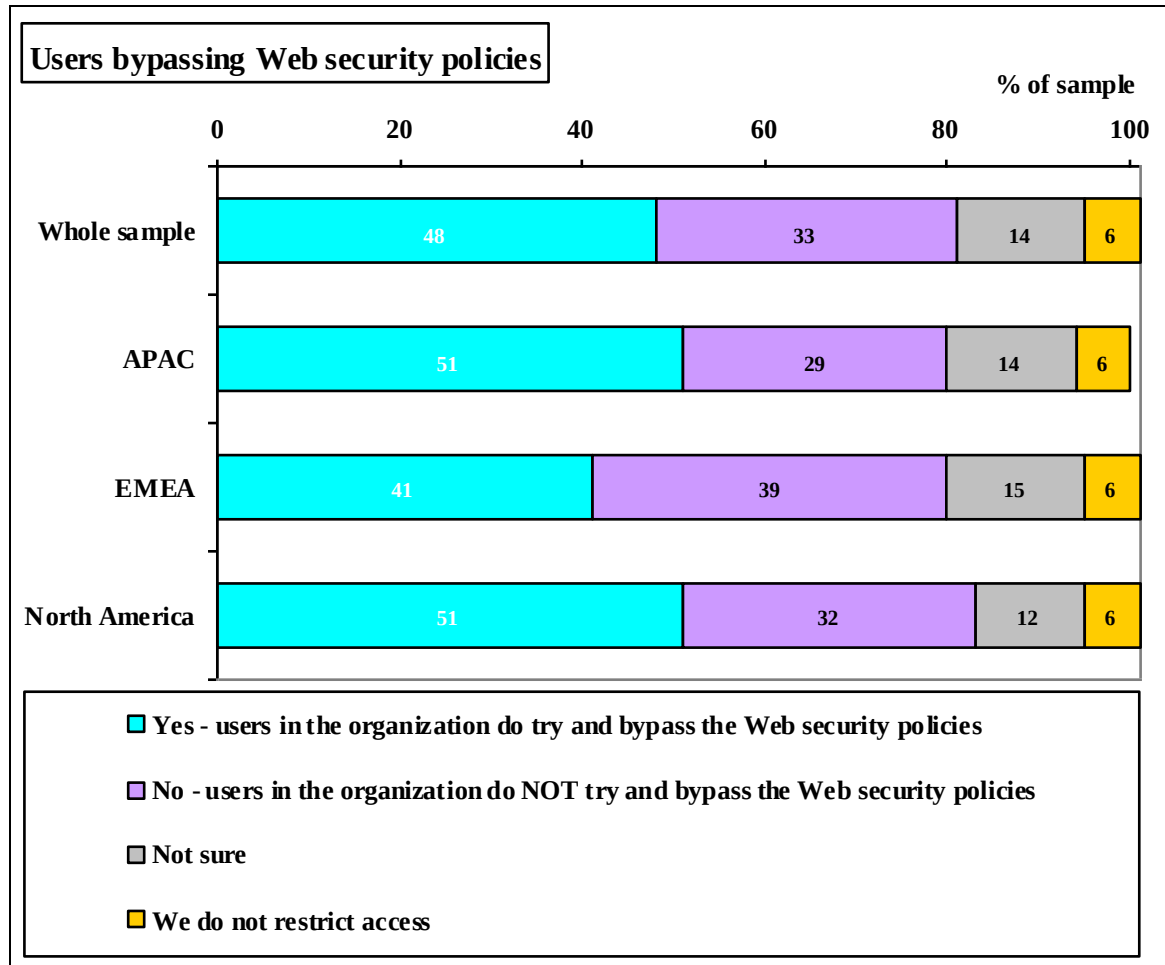
3.8. Are you under any pressure to include the following in your IT security strategy?



- Collectively, 90% of IT managers from around the world are under pressure to include at least 1 of these elements in their IT security strategy.
- In fact, 77% are under pressure to include multiple elements, and 38% are under pressure to include 5 or more [not shown].
- Two areas are slightly more common than others: protection from leakage of company confidential information (62%) and protection from inbound Web and email security threats (55%).
- But fewer than 1 in 2 are under pressure to build in regulatory compliance measures into their IT security strategy (49%), and the same is true for the protection of users' personal data (45%).

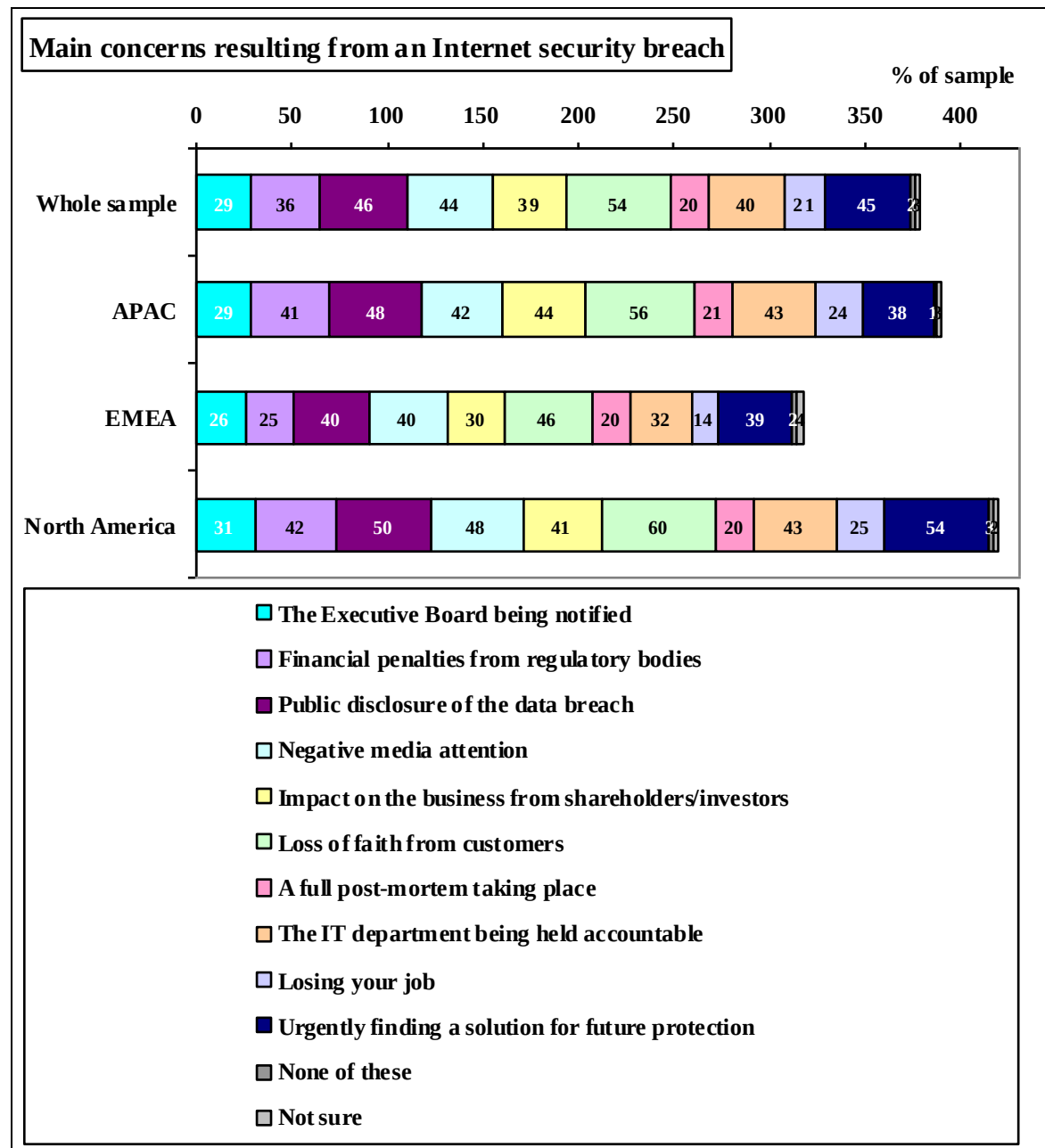
- In a similar vein, 43% are under pressure to demonstrate an understanding and identification of where confidential data resides for the company.
- But 45% of IT managers are under pressure to include something in their IT security strategy about how to empower and protect Internet users without being overly restrictive.
- Similarly, 41% are under pressure to include how to enable access to Web 2.0 sites without security worries.
- And as many (41%) are under pressure to include a means of keeping up with the ever-changing threat landscape in real-time.
- In contrast, just 5% of IT managers are not under pressure to include any of these areas in their IT security strategy.
- Another 5% are unsure which they are under pressure to include.
- Around the world, IT managers in North America are under pressure to include more of these in their IT security strategy, compared to the APAC and EMEA regions (i.e. length of the bars in the above chart).
- In more detail, more IT managers in North America (58%) are under pressure to include protection from inbound Web and email security threats, compared to the APAC region (50%).
- But more IT managers in the APAC (63%) and the North America (66%) regions are under pressure to include protection from leakage of company-confidential information, compared to the EMEA region (55%).
- Yet, more IT managers in North America (49%) are under pressure to demonstrate an understanding and identification of where confidential data resides for the company, compared to the APAC (39%) and EMEA (40%) regions.
- However, more IT managers in the EMEA (47%) and the North America (58%) regions are under pressure to build in regulatory compliance measures into their IT security strategy, compared to the APAC region (40%).
- Yet, more IT managers in North America (47%) are under pressure to include a means of keeping up with the ever-changing threat landscape in real-time, compared to the APAC (38%) and EMEA (36%) regions.
- And, more IT managers in North America (44%) are under pressure to include something about how to enable access to Web 2.0 sites without security worries, compared to the APAC (43%) and EMEA (36%) regions.
- And, more IT managers in North America (52%) are under pressure to include something in their IT security strategy about how to empower and protect Internet users without being overly restrictive, compared to the APAC (41%) and EMEA (39%) regions.

3.9. Do the users in your organization try and bypass your Web security policies?



- The research suggests that 94% of organizations have Web security policies in place in an attempt to restrict access.
- Yet 47% of IT managers say the users in their organization try and bypass their Web security policies.
- In contrast, 33% say the users do not behave in this way.
- Another 14% are not sure if users do this or not.
- But 6% say they do not restrict access via Web security policies.
- Around the world, more IT managers in the APAC and the North America regions (both 51%) say the users in their organization try and bypass their Web security policies, compared to the EMEA region (41%).
- Conversely, more IT managers in the EMEA region (39%) say the users in their organizations do not behave in this way, compared to the APAC (29%) and the North America (32%) regions.

3.10. If your company had an Internet security breach that resulted in data loss or had a significant and negative impact on the business, which of the following would you be concerned about?



- If an Internet security breach occurred that resulted in data loss or it had a significant and negative effect on the business, collectively 95% of IT managers would have concerns.
- From an internal perspective, 29% would be concerned about the Executive Board being notified, and another 20% would worry about a full post-mortem taking place.
- And 40% would worry about the IT department being held accountable, but 1 in 5 (21%) would actually be worried about losing their jobs.

- In terms of external perception, more (54%) would be worried about the inevitable loss of faith from customers.
- But fewer than 1 in 2 would be concerned about public disclosure of the data breach (46%), financial penalties from regulatory bodies (36%), the negative media attention that might follow (44%), and the impact on the business from shareholders / investors (39%).
- But only 45% would be concerned about urgently finding a solution for future protection.
- In contrast, 2% of IT managers say they would not be concerned about any of these issues, and another 3% are unsure which, if any, they would worry about.
- Around the world, IT managers in the APAC and North America regions would be concerned about more of these if an Internet security breach were to occur, compared to those in the EMEA region (i.e. length of the bars in the above chart).
- In fact, more IT managers in North America (80%) would have multiple concerns, compared to the EMEA region (74%) [not shown].
- In more detail, more IT managers in the APAC (41%) and North America (42%) regions would be concerned about financial penalties from regulatory bodies, compared to the EMEA region (25%).
- And, more IT managers in the APAC (48%) and North America (50%) regions would be concerned about public disclosure of the data breach, compared to the EMEA region (40%).
- Yet, more IT managers in North America (48%) would be concerned about the negative media attention that might follow, compared to the APAC (42%) and EMEA (40%) regions.
- But, more IT managers in the APAC (44%) and North America (41%) regions would be concerned about the impact on the business from any backlash from shareholders / investors, compared to the EMEA region (30%).
- And, more IT managers in the APAC (56%) and North America (60%) regions would be worried about the inevitable loss of faith from customers, compared to the EMEA region (46%).
- Also, more IT managers in the APAC and North America regions (both 43%) would worry about the IT department being held accountable, compared to the EMEA region (32%).
- In addition, more IT managers in the APAC (24%) and North America (25%) regions would actually be worried about losing their jobs, compared to the EMEA region (14%).
- But, more IT managers in North America (54%) would be concerned about urgently finding a solution for future protection, compared the APAC (38%) and EMEA (39%) regions.
- Finally, more IT managers in North America (3%) say they would not be concerned about any of these issues, compared to the APAC region (1%).

Appendix A: Quantitative Questionnaire

Qualifying questions

A) Does your organization have at least 250 PC users? [Select only 1]

- Yes [Continue]
- No [Terminate]

B) At which of the following IT management levels do you operate? [Select only 1]

- C-level (CIO) / director level [Continue]
- Manager level [Continue]
- Clerical / admin [Terminate]

Main questions

1) Which of the following statements represents how you feel about your company's Web security? [Select only 1]

- a) I'm confident that my company is 100% protected
- b) I'm confident I have as much protection as I need – some threats will always get in
- c) I am worried and frustrated this is not being addressed internally through lack of interest / budget / resources
- d) I am worried and know that we are overdue at addressing Web security
- e) I don't see this as an issue - why worry about Web security unless a problem occurs
- f) None of these
- g) Not sure

2) In addition to any firewall and antivirus solutions your organization has in place, does it have other specific solutions to do any of the following? [Select all that apply]

- a) Detect embedded malicious code on trusted Web sites
- b) Protect company-confidential data from being uploaded on the Web
- c) Real-time detection of malware
- d) Real-time prevention of malware entering your network
- e) URL filtering
- f) Prevent safe Web sites routing browsers to unknown sites
- g) Provide real-time analysis of Web site content
- h) Provide real-time Web content classification
- i) Stop spyware from sending out information to external sources
- j) Block phishing sites
- k) Block instant messaging attachments
- l) Control the use of USB devices
- m) None of these
- n) Not sure

3) Do you allow access to any of the following within your organization? [Indicate Yes/No/Not Sure for each]

- a) Social networks primarily used for personal use e.g. Facebook
- b) Social networks primarily used for business use e.g. LinkedIn
- c) Email services such as Hotmail, Yahoo, Gmail etc.
- d) Web portals such as iGoogle
- e) Auction sites
- f) Wikis
- g) Sites enabling users to upload video
- h) Sites enabling users to upload photographs
- i) Hosting services such as Yahoo! Geocities
- j) Hosted software/cloud computing such as Salesforce.com

- 4) Which of the following elements would you consider to be Web 2.0? [Indicate Yes/No/Not Sure for each]**
- a) Social networks primarily used for personal use e.g. Facebook
 - b) Social networks primarily used for business use e.g. LinkedIn
 - c) Email services such as Hotmail, Yahoo, Gmail etc.
 - d) Web portals such as iGoogle
 - e) Auction sites
 - f) Wikis
 - g) Sites enabling users to upload video
 - h) Sites enabling users to upload photographs
 - i) Hosting services such as Yahoo! Geocities
 - j) Hosted software/cloud computing such as Salesforce.com
- 5) Which of the following best describes your attitude to Web 2.0 sites and technology? [Select only 1]**
- a) Web 2.0 is necessary to our business – but it's a nightmare to manage
 - b) Web 2.0 is necessary to our business – it's not a problem to manage
 - c) Web 2.0 is not necessary to our business – we block all Web 2.0 sites
 - d) Web 2.0 is not necessary to our business – we do give users access to it
 - e) None of these
 - f) Not sure
- 6) Which one of the following areas of the Internet do you feel holds the most Web security threats? [Select only 1]**
- a) The 'dynamic' Web: Top 100 most popular sites (as ranked by Alexa)
 - b) The 'known' Web: Next 1 million sites (as ranked by Alexa)
 - c) The 'unknown' Web: The next 100 million sites (as ranked by Alexa)
 - d) No area of the Internet is safe – blended threats are everywhere in equal measure
 - e) Not sure
- 7) From which of the following groups within your organization do you feel pressure to allow access to Web 2.0 sites? [Select all that apply]**
- a) C-level / director level executive staff
 - b) IT
 - c) Marketing
 - d) Finance
 - e) HR
 - f) Sales
 - g) Users wanting personal time on Web 2.0 sites
 - h) Users wanting to use Web 2.0 sites for business
 - i) None of these
 - j) Not sure
- 8) Are you under any pressure to include the following in your IT security strategy: [Select all that apply]**
- a) Protection from inbound Web and email security threats
 - b) Protection from leakage of company-confidential information
 - c) Understanding and identification of where confidential data resides
 - d) Regulatory compliance
 - e) How to keep up with the ever-changing threat landscape in real-time
 - f) How to enable IT to allow Web 2.0 access without security worries
 - g) How to empower and protect Internet users without being overly restrictive
 - h) Protection of users' personal data
 - i) None of these
 - j) Not sure
- 9) Do the users in your organization try and bypass your Web security policies? [Select only 1]**
- a) Yes
 - b) No
 - c) Don't know

d) We do not restrict access

10) If your company had an Internet security breach that resulted in data loss or had a significant and negative impact on the business, which of the following would you be concerned about? [Select all that apply]

- a) The Executive Board being notified
- b) Financial penalties from regulatory bodies
- c) Public disclosure of the data breach
- d) Negative media attention
- e) Impact on the business from shareholders/investors
- f) Loss of faith from customers
- g) A full post-mortem taking place
- h) The IT department being held accountable
- i) Losing your job
- j) Urgently finding a solution for future protection
- k) None of these
- l) Not sure

- E N D -