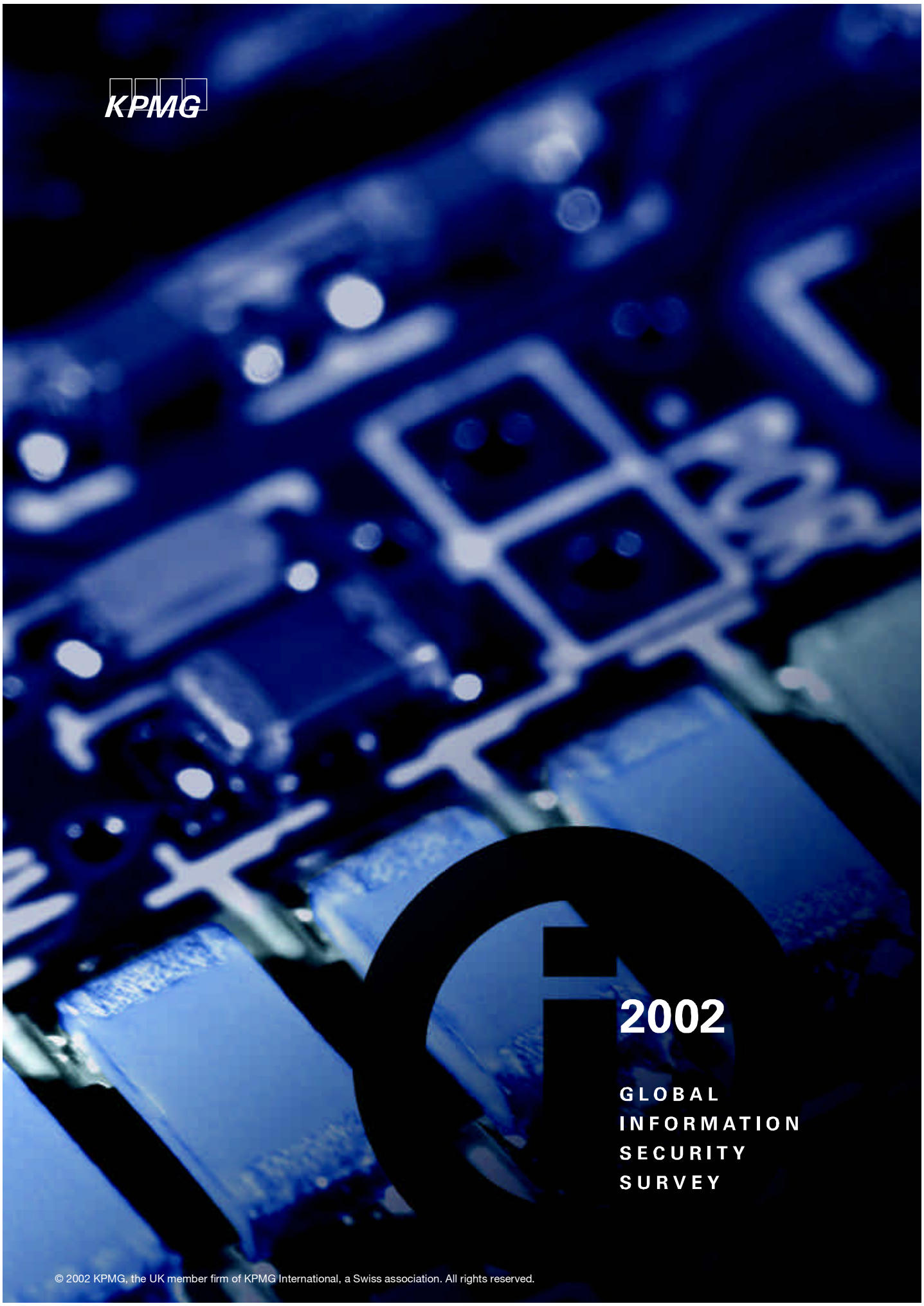


ExecutiveSUMMARY

A FIRST FOR KPMG

This is the first Global Information Security Survey undertaken by KPMG. We believe it will make a major contribution to knowledge and understanding of the information security problems that face every organization today, whatever their size or geographical range.

This belief is shared by the distinguished companies who have sponsored the survey – CheckPoint, RSA, Symantec and Secure Computing Magazine.

We set ourselves three principal tasks:

- evaluate the issues
- monitor how effectively organizations are addressing the well-known risks
- assess how prepared they are for those now emerging.

We carried out extended telephone interviews with senior managers responsible for information security in a cross-section of the world's largest organizations, those with a turnover greater than USD$50 million. The organizations selected covered all key business and government sectors in Europe, Middle East and Africa (EMEA), Asia/Pacific and the Americas.

Our main finding can be summed up in one phrase: Look for the weakest link.

In the world of e-business and extended enterprises, there are no effective geographical and organizational boundaries. If levels of Internet protection are not applied equally and everywhere, the weakest link will expose all others in the chain to attack.

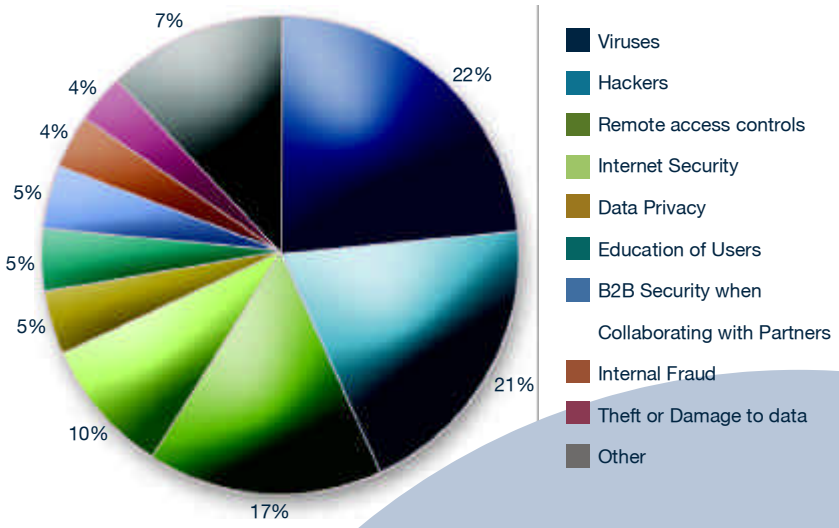
Because of the weakest link, because organizations are not as well protected as they think they are, because significant regional and market sector variations exist in levels of protection and because few organizations measure and report on security performance, millions of dollars are lost each year in security incidents. And down the drain with those dollars go customer confidence, the trust of business partners and opportunities that may never occur again.

THE FINDINGS - IN OUTLINE

Note:
We have defined information security as the practices, procedures and technology which ensure that information is safeguarded from unauthorized access, modification or accidental change, and is readily available to authorised users on request.

THE CRITICAL ISSUES

Respondents were asked what they thought were the most important security issues facing their organizations:.



BREACHES

Many organisations have experienced significant security breaches over the last year, as follows:

	Number of organisations reporting breaches	% suffering breaches	Average days lost/year	Average US$ lost/year	Highest reported US$ lost/year
Virus incident	390	61%	68	$162k	$10m
Theft of IT Equipment	246	38%	21	$98k	$3m
Email intrusion (eg.spamming)	183	29%	12	$16k	$0.2m
Loss of software	102	16%	19	$104k	$3m
Denial of service attack	91	14%	24	$53k	$0.5m
Website intrusion (eg. hacking)	79	12%	84	$32k	$0.2m
Critical system failure	79	12%	80	$155k	$4m
Loss of company documents (hardcopy)	78	12%	11	$37k	$0.2m
Loss of confidential data	35	5%	18	$197k	$1.5m
Tampering on input and output	23	4%	14	$14k	$0.1m

Prevention is better than cure. The average direct loss of all breaches suffered by each organization is USD$108,000. In addition there may be an opportunity cost of downtime and reduced employee productivity, and a further cost of improving security after the breach (which is usually far more costly than building security in at the outset). When you add in the long-term reputational damage that a security breach can have, the overall impact can be enormous. It is cheaper in the long run, and far less painful, to invest effectively to prevent a breach rather than to pick up the pieces and repair the damage after the event.

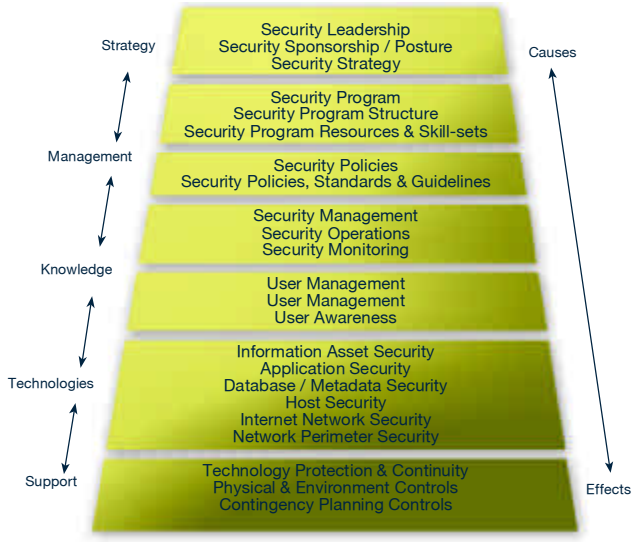
KPMG COMMENT

PROTECTION

We asked respondents to rate how well protected they thought they were from security-related threats. Perhaps not surprisingly almost all organizations (96 percent) thought that they were taking reasonable steps to protect themselves (58 percent strongly agree, 38 percent agree somewhat, 1 percent neither agree nor disagree, 2 percent disagree somewhat, 1 percent strongly disagree). However, when we compare these answers against the actual protection mechanisms employed, we found that many organizations are not as well protected as they think they are. Of those who said that they strongly agreed that they were reasonably protected:

- 10 percent do not test their security measures and therefore cannot know if these measures are effective in practice
- 52 percent have no form of intrusion detection system
- 87 percent have suffered some form of security breach this year, including:

a) 61% from Virus incidents
b) 28% form unwanted email intrusions
c) 15% from denial of service attacks
d) 13% from loss of software
e) 12% from Web site intrusion/hacking



An effective security environment requires comparable capabilities at all levels

Many organizations are over confident in the measures they use to protect themselves. The most successful adopt a layered security approach using a series of overlapping controls. Each control might only be 50% effective, but three or four of them working together can produce a greater level of security than one control can, even one that is 80% effective.

KPMG COMMENT

KPMG recommends an enterprise-wide architectural approach to security using a capability model (see above) which covers all areas of security within an organization.

KPMG COMMENT

For further information on related services or copies of the Global Information Security Survey CD, e-mail InformationSecurity@kpmg.com

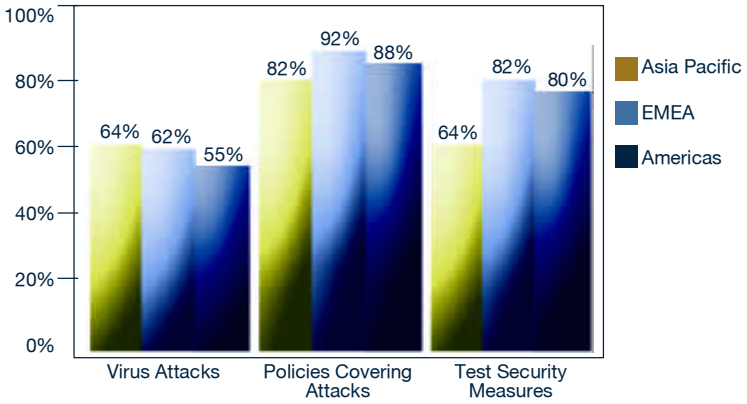
FIND THE WEAK LINK!

Respondents were asked where their organizations were based, whether they operated at a national, regional or global level, and in what market sectors. The answers to a number of questions were analysed to understand the levels of protection applied by different organizations around the world and in
the different sectors.

Organizations operating in Asia/Pacific and EMEA have a higher incidence of virus attacks (64 percent and 62 percent respectively) than those operating in the Americas (55 percent). However, fewer organizations in Asia/Pacific have policies covering virus incidents (Asia/Pacific 82 percent, EMEA 92 percent, Americas 88 percent) and fewer organizations in Asia/Pacific (64 percent) test their security measures to ensure that they are operating effectively (EMEA 82 percent, Americas 80 percent).

Financial sector organizations still lead the way in information security.

More financial sector (FS) organizations have implemented ISO 17799, the international standard on information security management (FS 25 percent, others 16 percent), more have intrusion detection systems (FS 44 percent, others 38 percent) and more measure the performance of security (FS 42 percent, others 33 percent). As a result, Financial Sectors have a lower level of security incidents in almost all areas than other sectors. e.g Virus attacks: FS 53 percent; others 63 percent and Web site intrusions/hacking: FS 9 percent; others 13 percent.



Threats are not focused simply on particular geographical or market sectors. Many hackers set automated tools to scan all possible IP addresses – disregarding location or line of business – to find vulnerabilities in systems.

Once they have found a vulnerability, they will look at the organization to determine if it is worth breaking into. If the organization is high profile, they may want to cause damage, or they may simply want to use a particular platform to launch another attack on a different organization and hide their tracks. Either way, the location and sector are unimportant – the threat is global.

KPMG COMMENT

PERFORMANCE

Only 43 percent of those responsible for information security could tell us how much was spent on information security this year and 30 percent of respondents did not know what percentage of the IT budget is spent on information security. In addition, only 60 percent of respondents have any form of security violation reporting. When asked whether their organization measures and reports on security performance, only 35 percent of respondents said that they did so now, and only a further 17 percent said they planned to in the future.

Measuring security performance is a growing area of concern. If you can't measure something, then you can't manage it effectively. Our survey results show that companies are lacking in ability to measure and report on security performance. How then do these organizations know that they are spending enough (and not too much) on protecting their systems and data and that they are getting value for money?

Security measures are important because they enable a company to track how well it is performing against specific efficiency, effectiveness and risk criteria. Without the ability to measure performance, a company cannot be sure that it really is protecting its information assets as well as it thinks it is.

KPMG COMMENT

Designed by Amorphous New Media