Information Security Survey 2004

March, 2005

Conducted by:

HKCERT

Technology Crime Division
Commercial Crime Bureau

Office of the Government
Chief Information Officer

Background

To better understand the information security status and trends in Hong Kong, an ongoing study is necessary to keep track of the extent of computer intrusions, the level of information security awareness, technologies adoption, security strategy employed and information security expense in Hong Kong.

This is the fifth time that such a study has been carried out. Four previous studies had been conducted on an annual basis since 2000. This report not only presents detailed findings from the current study but also compares with the previous results.

This study is jointly conducted by Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), Technology Crime Division of Commercial Crime Bureau of Hong Kong Police Force (HKPF) and Office of the Government Chief Information Officer (OGCIO) of The Government of the Hong Kong Special Administrative Region (HKSAR).

Objectives

The specific objectives of this study are to:

- Serve as an update of the previous studies.
- Identify the latest security technologies adopted by companies in Hong Kong.
- Investigate the types of computer attacks and their impacts.
- Understand the actions taken to deal with the attacks.
- Examine the security strategy adopted and the employment of information security staff.
- Investigate the companies' spending on information security.

Methodology

Sampling frame and criteria

Target sample units were registered companies in Hong Kong that utilized computers. Respondents were business decision makers, IT/MIS/EDP managers or people who took care of the computer systems.

Respondents were selected from 10 major industry sectors defined by Census & Statistics Department of HKSAR. Proportional sampling was adopted to ensure the distribution of the sample units by industry sector and staff size followed a similar pattern to that of the population.

Survey method

The previous questionnaire used in the 2003 survey was adopted in the current study. The questionnaire was also commented by HKCERT, HKPF, OGCIO and industrial professionals. In addition, pilot testing was undertaken internally to test the feasibility and ease of administration.

Telephone interview was adopted to gather the required information and a total of 3,000 questionnaires were completed between November and December 2004.

Quality assurance

To assure the quality of the data collected, all questionnaires were checked by independent people under several editing stages. Incomplete or doubtful cases were verified by follow-up calls.

Quality control techniques included cross-checking of data integrity and random call-back to the sample units. Data cleaning and verification by scientific measures were also implemented throughout the fieldwork and data analysis stages.

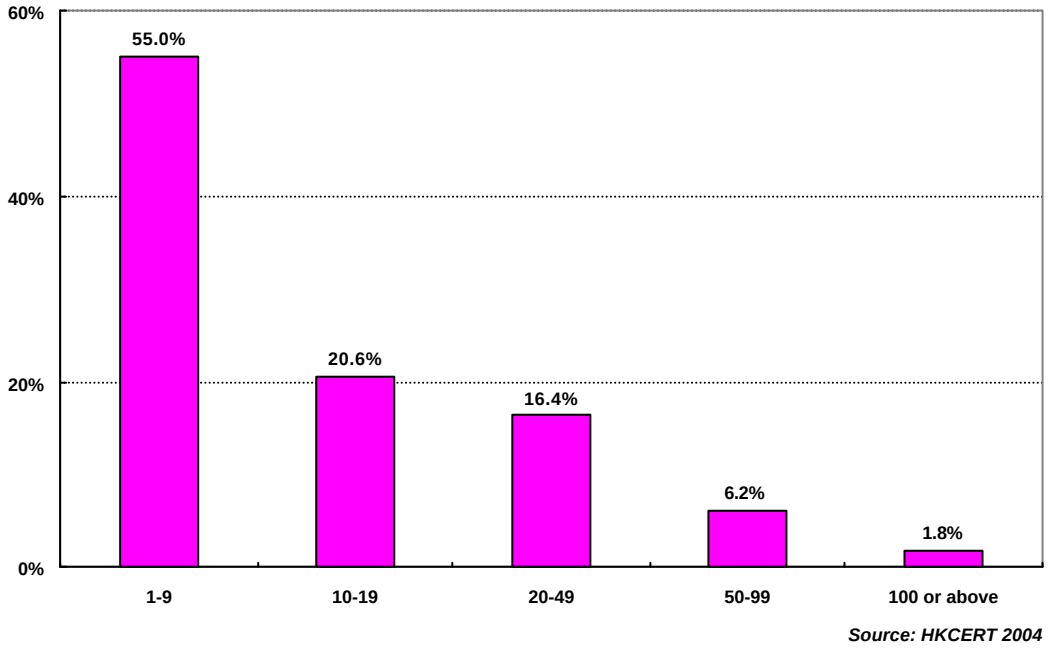
Sample demographics

Staff size

For easy reference and comparison, "small" companies in this report refers to companies employing less than 20 staff in Hong Kong, "medium-sized" companies hiring 20-99 staff and "large" companies employing 100 people or more.

As shown in Figure 1, three quarters of the surveyed companies (75.6%) were small enterprises and 22.6% of them were medium-sized enterprises. The remaining 1.8% were large organizations.

Figure 1: Staff size

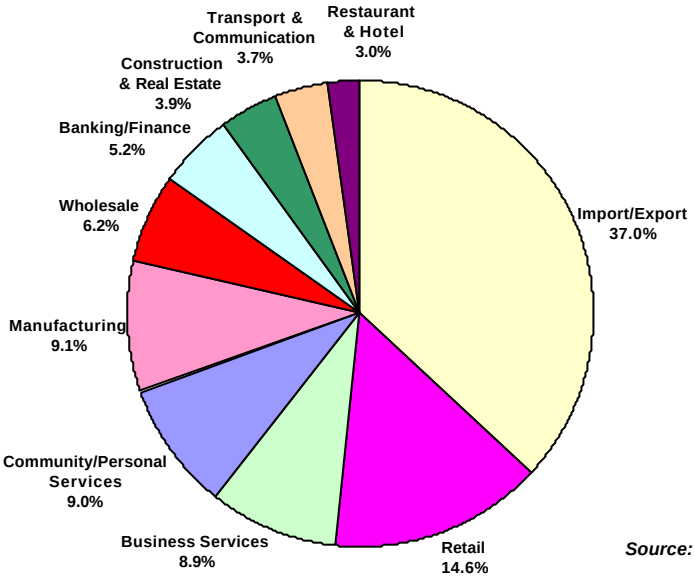


Source: HKCERT 2004

Industry sector

The distribution of the sample units by industry follows the spectrum of the population. The heaviest concentration of respondents was in the "Import/Export" sector (37%). "Retail" sector (14.6%) was the next largest industry segment (see Figure 2).

Figure 2: Industry sector



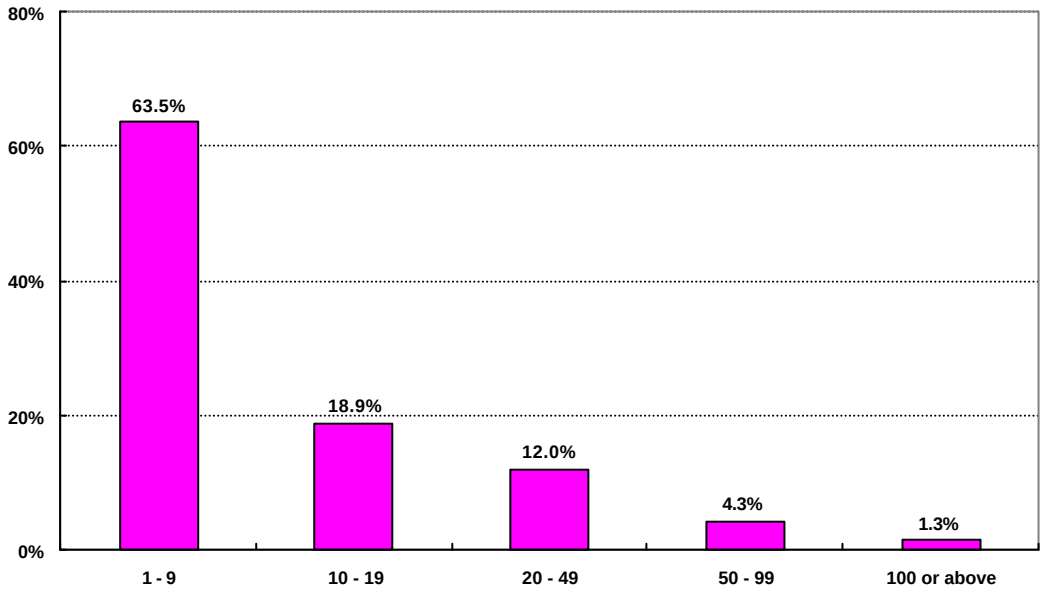
Source: HKCERT 2004

Major Findings

Number of PCs installed

The personal computer (PC) usage level skewed towards the low-end, largely owing to the dominance of small and medium-sized enterprises (SMEs) in the sample. Figure 3 illustrates that 63.5% of the surveyed companies had installed 1-9 PCs. Only 1.3% had installed 100 PCs or above.

Figure 3: Number of PCs installed



Source: HKCERT 2004

Security technology

As in previous studies, respondents were asked to identify the types of security technologies used in their companies. "Anti-virus software" was, again, the most popular security measure, being used by 90.9% of the companies interviewed in 2004 (see Figure 4). "Physical security" (65.5%), "Firewall" (65.4%) and "Password" (60.6%) were the next three common security measures adopted. The information security awareness of the companies in Hong Kong has increased considerably as the percentage of companies without any security measures in place dropped from 10.1% in 2003 to 3.6% in 2004. A detailed comparison of the security technologies used in the surveyed companies from 2000 to 2004 is attached in Appendix I.

The use of firewall increased significantly in 2004. There may be two reasons behind. Firstly, an increasing number of companies find the basic security tools like anti-virus software cannot completely stop virus or other computer attacks so they install firewalls to further protect their computer systems. Secondly, software vendors pay great effort in promoting the use of firewall. For instance, firewall will be automatically turned on if Windows XP Service Pack 2 is being applied.

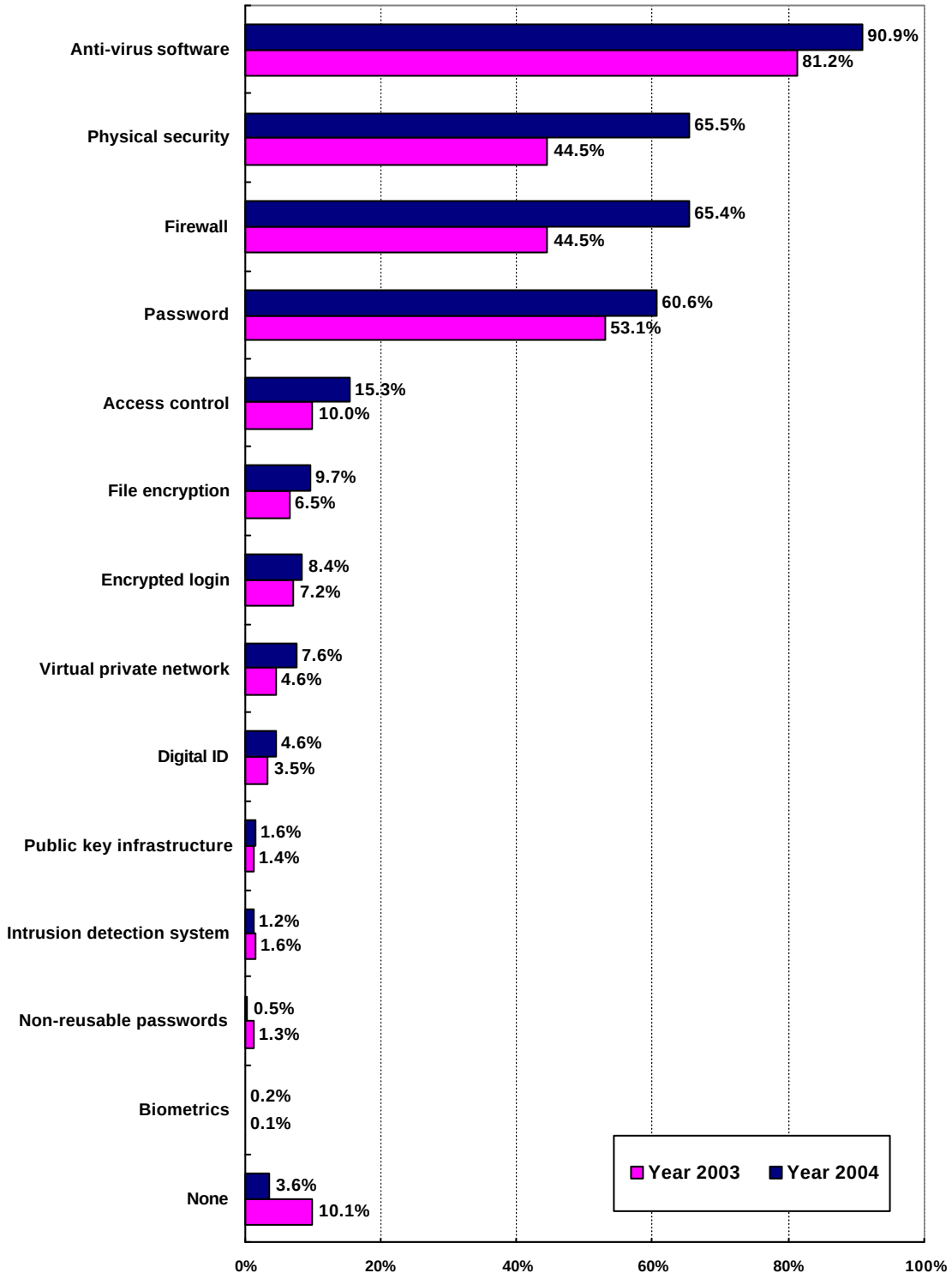
It is also noted that more companies adopted firewall than a basic technology – password in 2004. This indicates that firewall becomes basic. Many companies consider that firewall is an essential information security technology to protect their computer systems.

Table 1 demonstrates the security technologies deployed by staff size. Large companies are likely to use more and wider range of security measures.

In addition, the adoption rate of the security technologies has improved. In 2004, each small firm adopted 2.9 security measures on average whereas the figure for medium companies was 4.7. These numbers were larger than the respective values in 2003.

For large enterprises, the average number of security measures also increased slightly from 5.3 in 2003 to 5.9 in 2004.

Figure 4: Security technologies adopted (2003-2004)



Source: HKCERT 2004

Table 1: Security technologies adopted by staff size (2003-2004)

	1-19		***20-99***		***100 or above***	
	2003	**2004**	**2003**	**2004**	**2003**	**2004**
Anti-virus software	78.2%	89.8%	91.7%	94.4%	92.9%	92.5%
Password	46.6%	54.6%	76.3%	78.8%	76.2%	86.8%
Physical security	40.6%	61.6%	58.7%	77.0%	57.1%	84.9%
Firewall	38.5%	60.7%	64.3%	79.1%	85.7%	92.5%
Access control	4.4%	5.7%	28.2%	42.9%	57.1%	73.6%
File encryption	3.5%	4.2%	15.9%	26.0%	33.3%	34.0%
Encrypted login	3.7%	3.9%	19.3%	21.7%	28.6%	32.1%
Virtual Private Network	1.2%	1.8%	14.7%	24.0%	40.5%	45.3%
Intrusion detection system	1.0%	0.3%	3.6%	3.7%	7.1%	11.3%
Digital ID	1.7%	2.2%	9.1%	11.5%	19.0%	17.0%
Public Key Infrastructure	0.7%	0.4%	3.4%	5.2%	9.5%	9.4%
Non-reusable passwords	0.3%	0.1%	3.9%	1.3%	16.7%	5.7%
Biometrics	0%	0.1%	0.5%	0.3%	2.4%	1.9%
None	12.1%	4.4%	3.1%	1.3%	2.4%	0%
Total	**232.5%**	**289.6%**	**392.7%**	**467.1%**	**528.6%**	**586.8%**
Average number of security measures per company	***2.3***	***2.9***	***3.9***	***4.7***	***5.3***	***5.9***

Security level

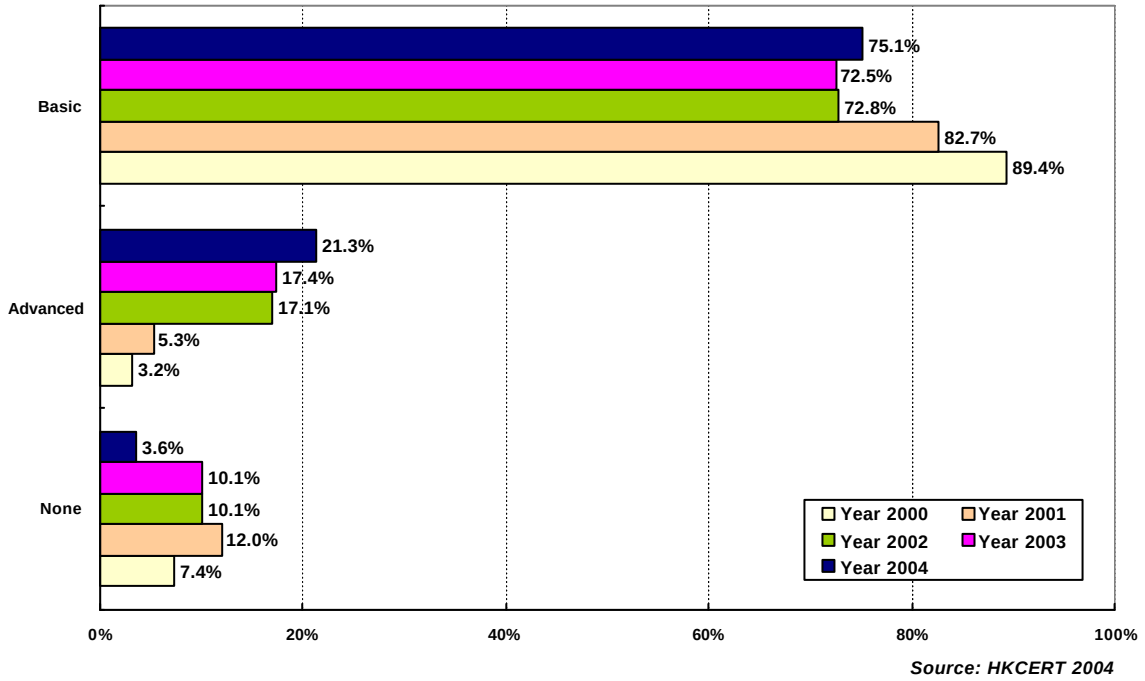
Like previous studies, interviewed companies are grouped into different security levels for further analytical purposes. However, as firewall becomes a basic security technology, only three security levels, namely "None", "Basic" and "Advanced" are defined this year. Detailed classifications are listed in Table 2.

Table 2: Classification of security technologies

Security Level	***Types of security technology adopted***
None	No use
Basic	Anti-virus software/Password/Physical security/Firewall only
Advanced	File encryption/Access control/Intrusion detection system/Virtual private network/Encrypted login/Non-reusable passwords/Digital ID/Public key infrastructure/Biometrics *with/without* Basic security technologies

Figure 5 shows the security level of the surveyed companies for the 2000-2004 period. It reveals that increasingly more companies are using Advanced level of security measures to safeguard against computer attacks. Slightly more than one-fifth of the surveyed companies (21.3%) belonged to the Advanced security level in 2004 while the percentage was only 17.4% in 2003.

Figure 5: Security level (2000-2004)



Source: HKCERT 2004

The security level correlates with the staff size. More large enterprises (88.7%) utilized Advanced security technologies to prevent security breaches than medium-sized companies (55.6%) and small entities (9.5%) in 2004 (see Table 3).

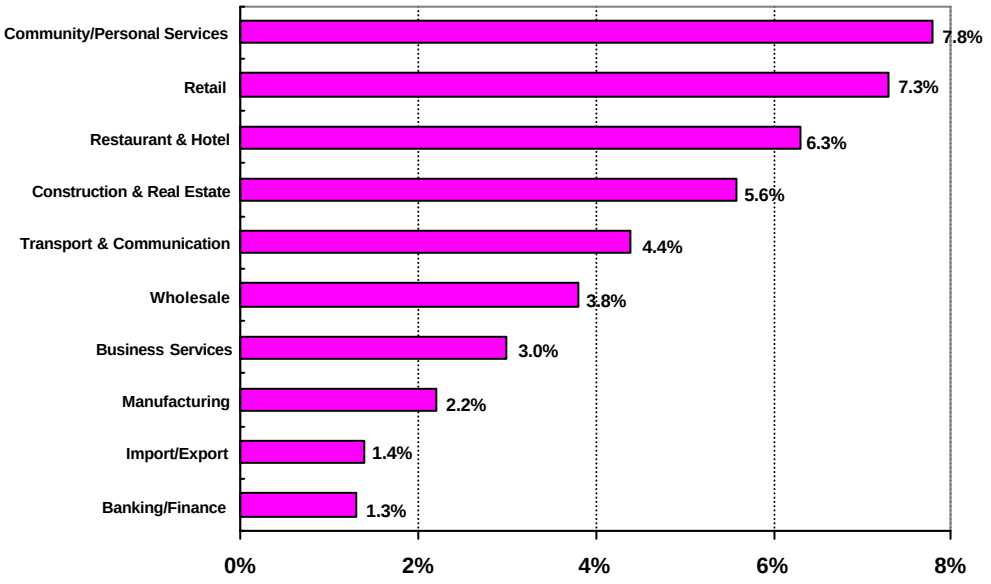
Overall speaking, the security level has greatly improved in 2004. The percentage of small companies not using any security technologies dropped significantly from 12.1% in 2003 to 4.4% in 2004. Nonetheless, companies should continue to improve their security technologies to protect their computer systems.

Table 3: Security level by staff size (2003-2004)

	1-19		*20-99*		*100 or above*	
	2003	**2004**	**2003**	**2004**	**2003**	**2004**
None	12.1%	4.4%	3.1%	1.3%	2.4%	0%
Basic	79.1%	86.1	50.7%	43.1%	26.2%	11.3%
Advanced	8.8%	9.5%	46.2%	55.6%	71.4%	88.7%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Cross-industry analysis indicates that relatively more companies in "Community/Personal Services" (7.8%) and "Retail" (7.3%) sectors did not use any security technologies.

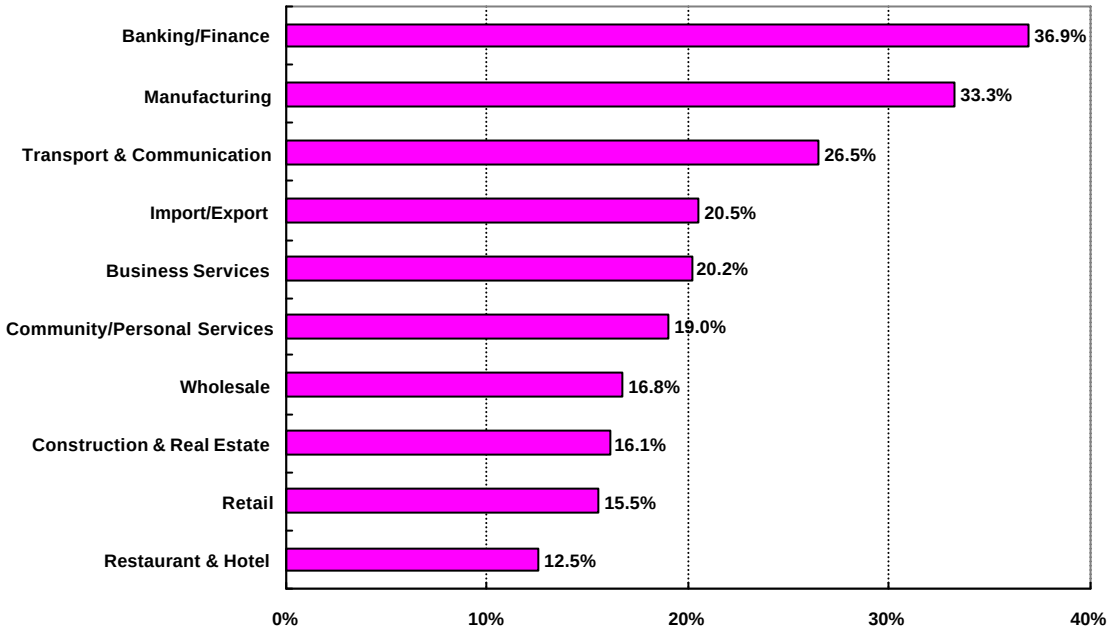
Figure 6: No security technologies in place by industry sector



Source: HKCERT 2004

On the other hand, "Banking/Finance", "Manufacturing" and "Transport & Communication" sectors were better prepared for the attacks, with 36.9%, 33.3% and 26.5% adopting Advanced security technologies correspondingly (see Figure 7).

Figure 7: Advanced security level by industry sector



Source: HKCERT 2004

Computer attacks

The current study shows that slightly over three-fifths of the interviewed companies (61.3%) had installed servers and/or web sites. Of these companies, 17.7% (326 out of 1,839 companies) had experienced computer attacks within the last 12 months. Fifty two percent of the victimized companies reported 2-4 incidents and 34% mentioned once.

The total number of incidents recorded in the sample decreased from 943 incidents in 2003 to 865 incidents in 2004, down by 8.3% (see Table 4). The decrease in number of computer attacks can be attributed to the improved security technologies deployed.

On the other hand, the average number of attacks per victimized company increased slightly from 2.4 in 2003 to 2.7 in 2004.

Table 4: Total number of incidents and average number of attacks per victimized company

	2000	**2001**	**2002**	**2003**	**2004**
Total no. of incidents	1,510	1,387 *(-8.1%)*	1,095 *(-21.1%)*	943 *(-13.9%)*	865 *(-8.3%)*
Average no. of attacks per victimized company	2.6	3.5 *(+34.6%)*	3.4 *(-4%)*	2.4 *(-29.4%)*	2.7 *(+12.5%)*

The seriousness of computer attacks also decreased (see Table 5). Both the total number of PCs affected and average number of PCs affected per incident continued to drop in 2004 after reaching a peak in 2002.

A total of 3,464 PCs were affected in 2004, down by 15.5% from 2003. In addition, the average number of PCs affected per incident dropped from 4.3 in 2003 to 3.9 in 2004.

Table 5: Total number of PCs affected and average number of PCs affected per incident

	2000	**2001**	**2002**	**2003**	**2004**
Total no. of PCs affected	4,733	5,366 *(+13.4%)*	5,460 *(+1.8%)*	4,098 *(-24.9%)*	3,464 *(-15.5%)*
Average no. of PCs affected per incident	3.1	3.9 *(+25.8%)*	5 *(+28.2%)*	4.3 *(-14%)*	3.9 *(-9.3%)*

To further examine the impact of computer attack, the average number of PCs affected per incident and the impact per computer attack by staff size were calculated.

Average PCs affected per incident (APC) = Total PCs affected/Total no. of incidents

Impact per computer attack (IPC) = Average [APC/Total PCs in a company]

Table 6: Extent and impact of computer attack (2000-2004)

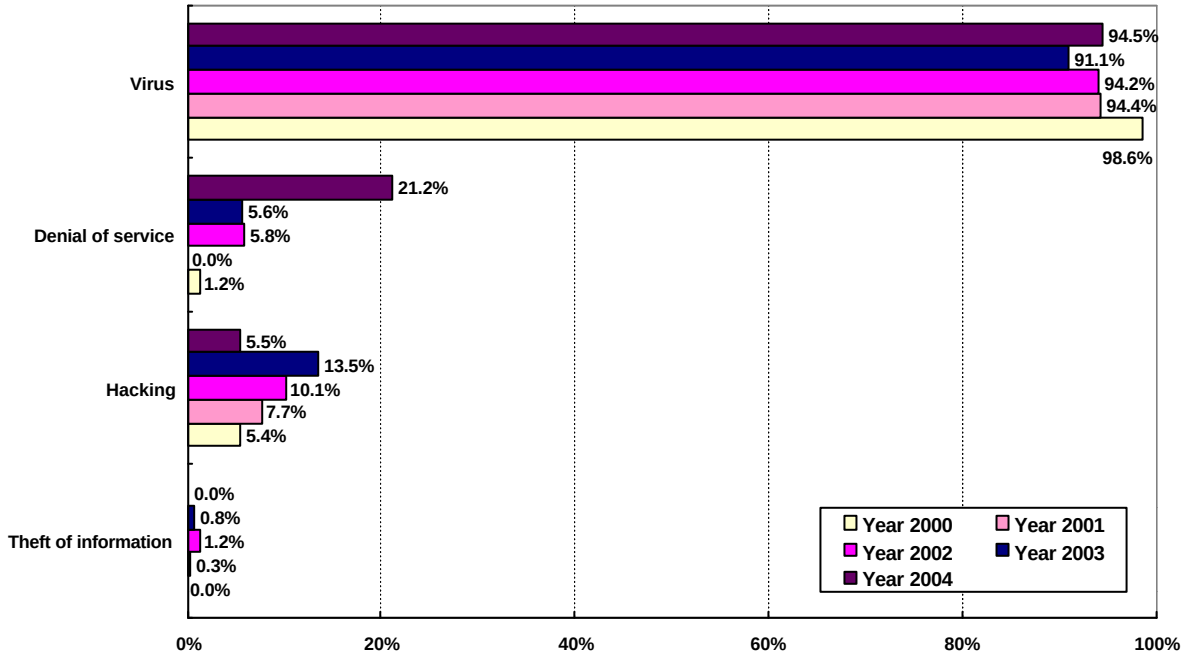
	Average PCs affected per incident					***Impact per computer attack***				
Staff size	**2000**	**2001**	**2002**	**2003**	**2004**	**2000**	**2001**	**2002**	**2003**	**2004**
1-19	2.2	2.9	3.4	3.4	3.2	0.34	0.35	0.46	0.43	0.45
20-99	3.8	6.2	8.0	5.2	5.9	0.18	0.20	0.31	0.23	0.25
100 or above	10.9	13.7	16.5	10.8	8.7	0.09	0.11	0.31	0.11	0.09

Table 6 shows that the average number of PCs affected per incident increases with company size. In terms of the impact per computer attack, it is found that small companies suffered a much larger impact than medium-sized or large companies. Specifically, in 2004, impact per computer attack on small companies was 0.45 while the impact on medium-sized companies and large companies were relatively low, with the figures of 0.25 and 0.09 accordingly.

Figure 8 shows the types of computer attack detected by the surveyed companies in the last 12 months. Computer virus (94.5%) was still the most prevailing form of computer attack in 2004, followed by denial of service (21.2%) and hacking (5.5%). Compared with the figures in 2003, the percentage of denial of service increased and the percentage of hacking decreased in 2004.

The sharp increase in the denial of service attack may be due to the increase in the number of virus threats such as the numerous variants of the Netsky, Bagel and MyDoom worms which generate a lot of messages on the Internet, creating denial of service effect. This kind of attack respondents mentioned was, basically, not intentional. Typically, it only creates traffic busy and victimized companies will experience temporary loss of network connectivity and services. For example, a web site of a victimized companies is accessed by thousands of people at the same time can be forced to temporarily cease operation.

Figure 8: Types of computer attack (2000-2004)



n = companies suffered from computer attacks in the last 12 months ***Source: HKCERT 2004***

Table 7 compares the respondents' estimates of the financial losses caused by different types of computer attack. Virus remained the dominant type of attack and accounted for 80.2% of the monetary loss, equivalent to a sum of HK$0.68 million in 2004. The financial losses due to hacking and denial of service were HK$42,150 and HK$0.13 million respectively.

The magnitude of financial losses further declined in 2004. In the current study, a sum of HK$0.85 million was recorded among those companies that suffered from computer intrusions, down from HK$1.22 million in 2003. This is a positive signal that companies have taken faster actions to deal with the attacks once they are discovered and pay more efforts to minimize the impact of the attacks.

Table 7: Financial losses by type of computer attack within the last 12 months (2000-2004)

	Total financial loss (HK$)				
Type of computer attack	**2000**	**2001**	**2002**	**2003**	**2004**
Virus	1,259,650	1,446,500	1,352,483	819,550	684,150
Denial of service	0	0	96,500	32,850	126,850
Hacking	116,000	77,500	206,900	286,000	42,150
Theft of information	0	0	180,000	83,000	0
Total	**1,375,650**	**1,524,000** ***(+10.8%)***	**1,835,883** ***(+20.5%)***	**1,221,400** ***(-33.5%)***	**853,150** ***(-30.1%)***
Average Financial Loss per Victimized Company	**2,461**	**3,888** ***(+58%)***	**5,632** ***(+44.9%)***	**3,116** ***(-44.7%)***	**2,617** ***(-16%)***

In this survey, 38.5% of respondents reported that the incidents had resulted in financial losses in 2004, up by 18.1% from 2003 (see Table 8).

The drop in financial losses can be explained by the decrease in the total number of incidents and the number of PCs affected. However, the losses might be underestimated as some companies failed to quantify the financial impact. For instance, they had not taken manpower and time costs to fix the systems and intangible costs such as ruin of image into consideration.

Table 8: No. of incidents by type of computer attack within the last 12 months (2000-2004)

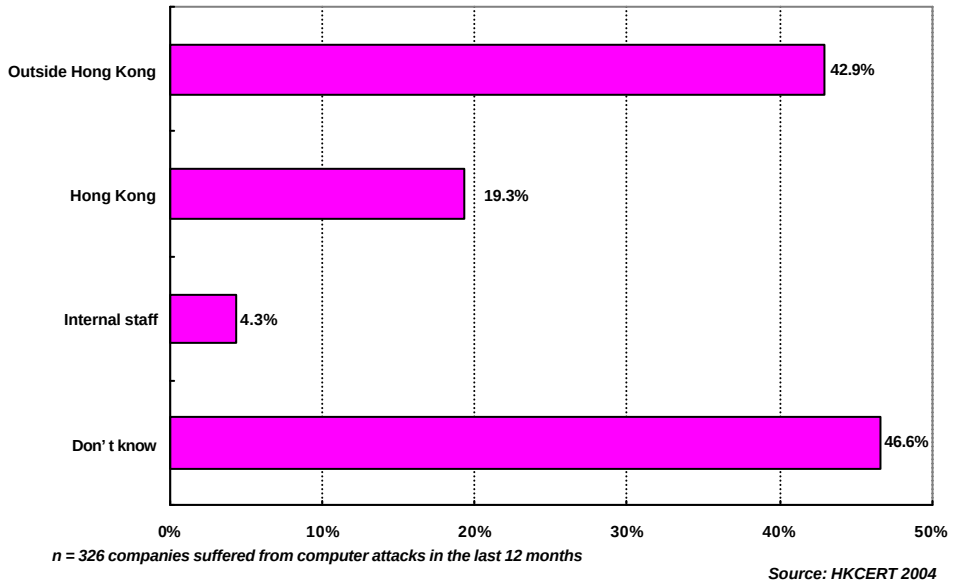
Type of computer attack	*No. of incidents*				
	2000	**2001**	**2002**	**2003**	**2004**
Virus	551	370	307	357	305
Denial of service	7	0	19	22	69
Hacking	30	30	33	53	16
Theft of information	0	1	4	3	0
Total	**588**	**401**	**363**	**435**	**390**
% of incidents reported financial loss	**13.3%**	**37.4%**	**54%**	**32.6%**	**38.5%**

Sources of attack

This report identified three main sources of computer attack, namely outside Hong Kong, Hong Kong and internal staff. The survey results show that 42.9% of the attacks were from overseas while 19.3% were from Hong Kong.

It should be noted that a lot of respondents (46.6%) did not know the origin of the attacks. As computer intrusions can take place at any time, from anywhere and by anyone, companies should not just take passive measures to fix the loopholes of their computer systems after the attacks. They should also take proactive actions to protect confidential company information and investigate the source of attacks to prevent recurrence. Understanding the sources of attack can help formulate a better security strategy.

Figure 9: Sources of attack



n = 326 companies suffered from computer attacks in the last 12 months

Source: HKCERT 2004

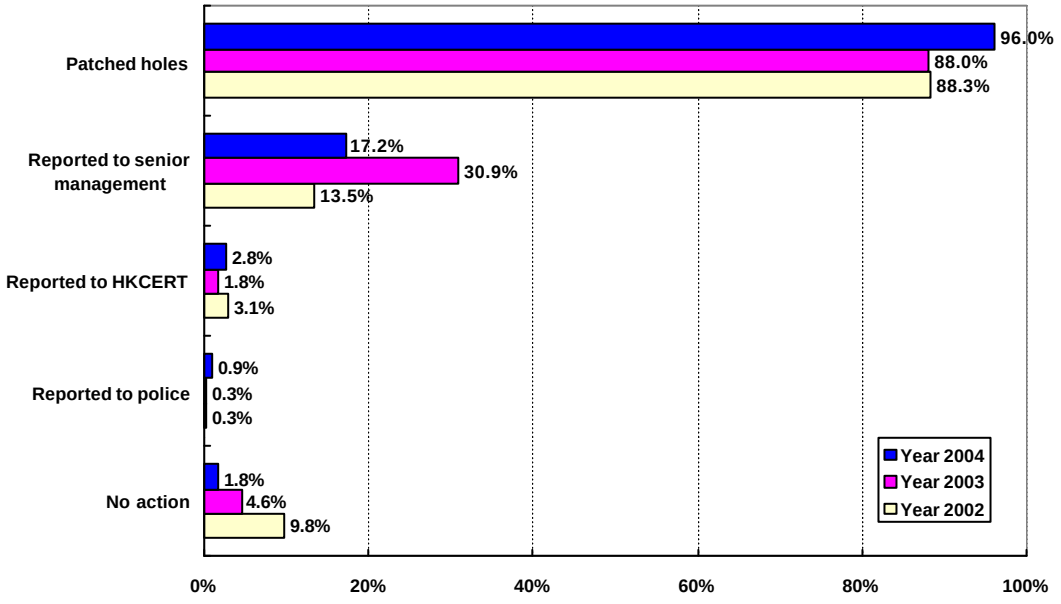
Actions against computer attacks

Figure 10 compares the interviewed companies' responses to computer attacks for 2002-2004. The high percentage of patching security holes (96%) and a noticeable decline in the percentage of "no action" in 2004 reflects that increasingly more companies are aware of the consequences of computer attacks to their business and have taken remedial actions.

Close to one-fifth of respondents expressed that they would report to senior management (17.2%). The percentage dropped substantially when compared with the percentage in 2003. It may be due to the fact that many companies have already experienced computer attacks, the information security staff themselves can deal with the attacks and do not need to report the attacks to their senior management anymore.

Only 2.8% and 0.9% of the respondents would report the company attacks to HKCERT and police respectively.

Figure 10: Actions against computer attacks (2002-2004)



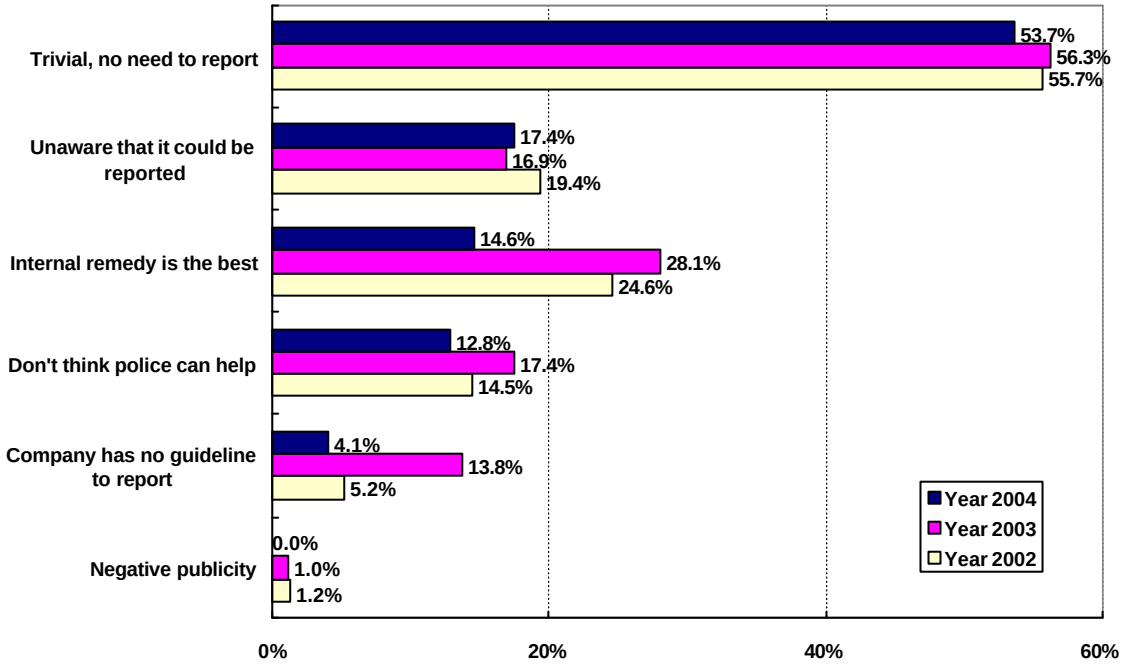
n = companies suffered from computer attacks in the last 12 months

Source: HKCERT 2004

The major reason for not reporting to the police was found to be "Trivial, no need to report" (53.7%), followed by "Unaware that it could be reported" (17.4%), "Internal remedy is the best" (14.6%) and "Don't think police can help" (12.8%).

The high percentage in "Trivial, no need to report" is due to the fact that most of the computer attacks detected by the interviewed companies were virus incidents that normally did not involve theft of company information or serious computer crimes. So, responded companies did not need to report to police.

Figure 11: Reasons for not reporting to police (2002-2004)

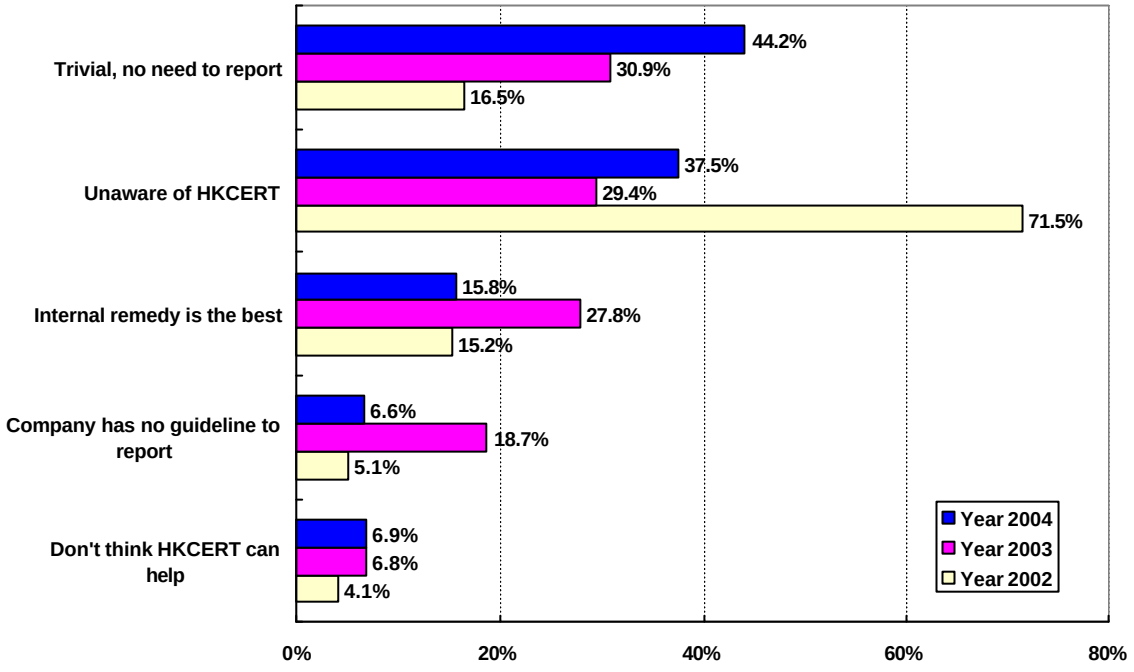


n = companies who had not reported to police after computer attacks

Source: HKCERT 2004

Figure 12 summaries the reasons why the surveyed companies did not report the computer attacks to HKCERT. Slightly over two-fifths of respondents (44.2%) considered that the attacks were trivial and did not need to be reported. Being unaware of HKCERT (37.5%) and believing in internal remedy was the best (15.8%) were also two other more frequently quoted answers.

Figure 12: Reasons for not reporting to HKCERT (2002-2003)



n = companies who had not reported to HKCERT after computer attacks *Source: HKCERT 2004*

Security management

As in the previous study, some questions regarding security management were included to check if the respondents' companies have taken any proactive measures to improve computer security on top of the use of security technologies. Security management in this survey covers four aspects, including information security risk assessment and audit, information security policy, incident response procedures and regularly applying security patches.

It seems that many surveyed companies still have not taken enough initiatives in preventing or tackling computer intrusions. The percentages of surveyed companies that had information security risk assessment and audit, information security policy and incident response procedures in place were still low in 2004, with only 11.6%, 18.1% and 22.6% respectively (see Table 9). Notwithstanding that, more companies applied security patches regularly to safeguard their computer systems in 2004 when compared with the figure in 2003. As most of the incidents were caused by vulnerabilities, applying patch is the suitable solution.

In general, large companies are more proactive in implementing a comprehensive security management strategy than SMEs.

The survey findings may reflect the fact that many companies, especially SMEs, do not invest too much in security management. Instead, they prefer to use measures that are free of charge and easy to implement, such as applying security patches.

Table 9: Security management in place (2003-2004)

Staff size	**Information security risk assessment and audit**		**Information security policy**		**Incident response procedures**		**Regularly applying security patches**	
	2003	**2004**	**2003**	**2004**	**2003**	**2004**	**2003**	**2004**
1-19	8.3%	6.8%	11%	11.2%	20.5%	16.0%	47.2%	56.9%
20-99	25.3%	25.2%	38.6%	37.9%	46.2%	42.2%	73.3%	79.4%
100 or above	57.1%	41.5%	57.1%	60.4%	69.0%	58.5%	85.7%	90.6%
All companies	**12.5%**	**11.6%**	**17.3%**	**18.1%**	**26.5%**	**22.6%**	**53.1%**	**62.6%**

The percentage of companies that had already implemented information security policy increased slightly from 17.3% in 2003 to 18.1% in 2004. Tables 10 and 11 compare the implementation rate of information security policy from 2002 to 2004 by staff size and by industry sector respectively.

Table 10: Implementation of information security policy by staff size (2002-2004)

Staff size	**2002**	**2003**	**2004**
1-19	9.5%	11.0%	11.2%
20-99	30.8%	38.6%	37.9%
100 or above	58.8%	57.1%	60.4%
All companies	**14.2%**	**17.3%**	**18.1%**

Table 11: Implementation of information security policy by industry sector (2002-2004)

Industry sector	**2002**	**2003**	**2004**
Banking/Finance	30.4%	30.8%	35.7%
Restaurant & Hotel	20.6%	17.6%	17.2%
Manufacturing	18.2%	22.4%	21.2%
Business Services	16.3%	22.8%	26.6%
Community/Personal Services	14.2%	19.3%	20.8%
Import/Export	13.4%	16.7%	15.5%
Transport & Communication	11.9%	20.0%	23.0%
Retail	10.6%	12.3%	11.2%
Construction & Real Estate	9.7%	6.9%	12.9%
Wholesale	7.7%	12.2%	15.1%
All sectors	**14.2%**	**17.3%**	**18.1%**

Information security staff

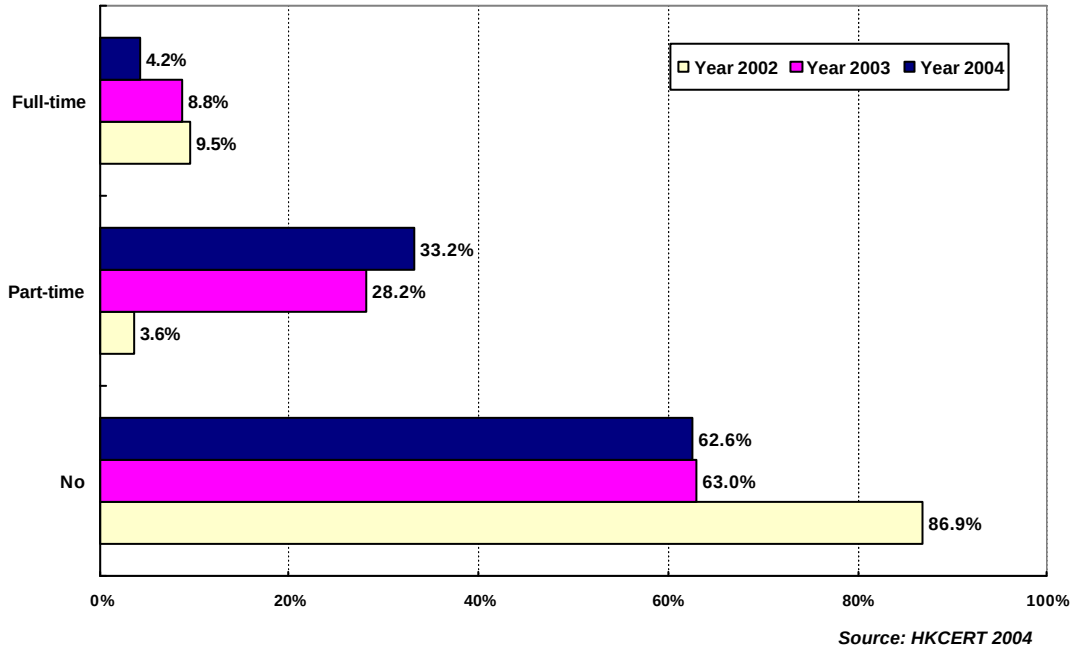
Close to two-fifths of the surveyed companies (37.4%) employed full-time or part-time staff to deal with information security issues (see Figure 13). The ratio is more or less the same as that in 2003.

In specific, the percentage of in-house full-time information security staff decreased but the part-time staff increased in 2004. It can be explained by the fact that many companies have taken more preventive actions such as deploying more or higher levels of information security technologies, they then relatively adopt less reactive measures such as delegating more manpower to look after the computer systems.

Moreover, as many companies have the experience to handle computer attacks and know how to deal with the attacks once detected, the workload for the information security maintenance may drop. Companies, then, prefer to employ someone who can take care of their computer systems on a part-time basis.

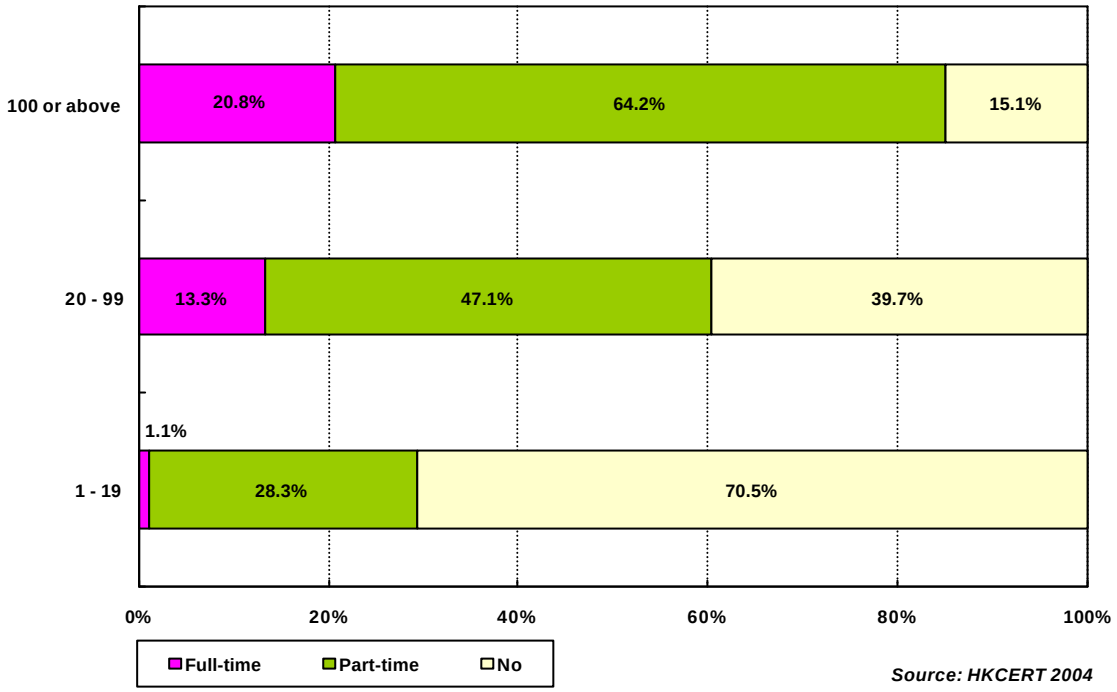
Large companies are more inclined to employ delegate persons to look after their systems to prevent computer attacks. Figure 14 shows that 85% of the large companies had full-time or part-time staff responsible for information security whereas only 29.4% of small enterprises hired information security staff.

Figure 13: In-house information security staff (2002-2004)



Source: HKCERT 2004

Figure 14: In-house information security staff by staff size



Source: HKCERT 2004

Information security expense

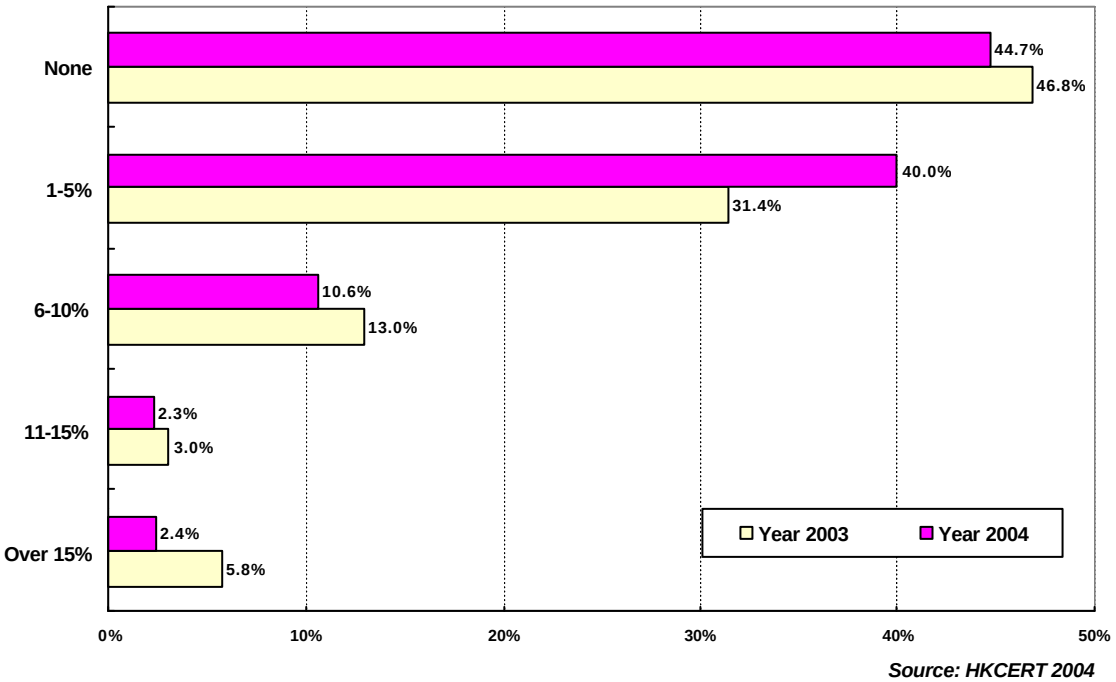
Slightly more than two-fifths of the surveyed companies (44.7%) did not spend on information security in the last 12 months (see Figure 15). On the other hand, 40% of sample units reported that 1-5% of their annual IT expenditure were spent on information security. Only 2.4% had spent over 15% of their annual IT expenses on information security.

It is noted that the share of annual IT expenditure on information security decreased in 2004. On average, only 3.1% of the annual IT expense was allocated to information security in 2004 as compared to 4.3% in 2003. One of the reasons may be that many companies have already purchased software and equipment for the information security purposes. By economies of scale, spending on information security will be less.

Among those companies that reported no expenses on information security, their reasons were:

- No information security technologies had been deployed.
- Information security spending could not be separated from the IT spending.
- No information security expense was incurred in 2004.
- Using free information security measures.

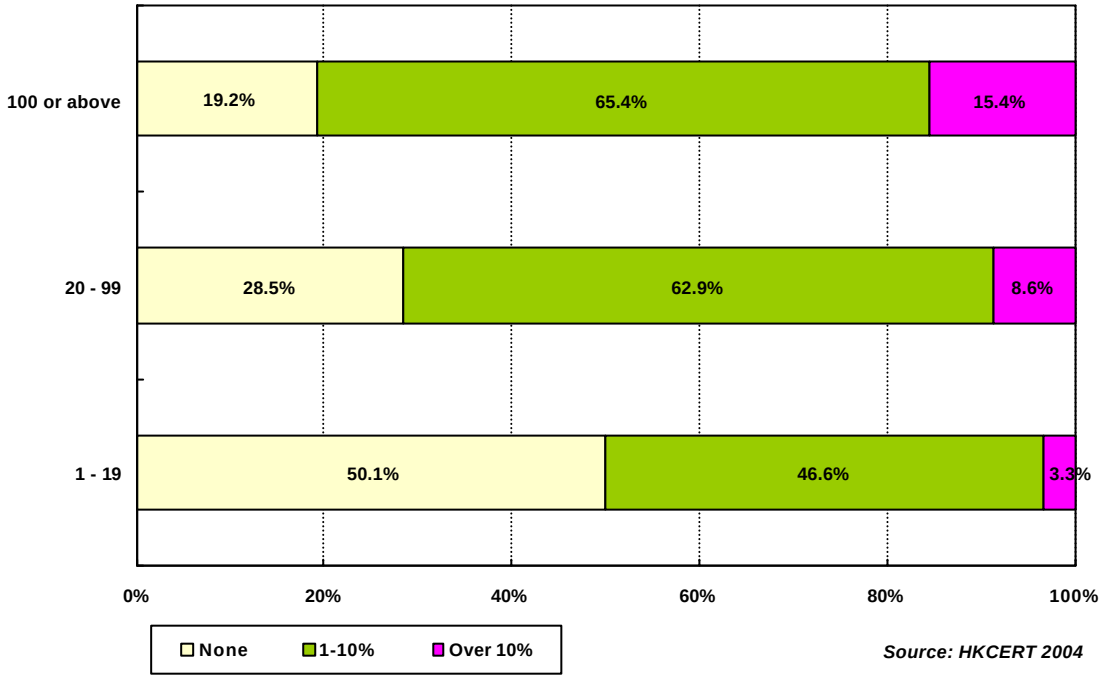
Figure 15: Information security expense (2003-2004)



Source: HKCERT 2004

The percentage of IT spending allocated to information security shows a positive relationship with the company size. Larger companies tend to have a higher spending ratio on information security (see Figure 16).

Figure 16: Information security expense by staff size



Conclusions

Information security in Hong Kong has been improved. More companies adopt more and higher level of security measures and software vendors provide better countermeasures than before. In addition, the seriousness of computer attacks decreased in 2004. The current survey shows that the total number of computer intrusions, total financial loss and total number of PCs affected dropped.

It is found from the survey findings that firewall becomes a basic information security measure. Sixty-five percent of the surveyed companies used firewall in 2004. Moreover, applying security patch is also an easy and suitable solution to prevent intrusion attempts as most computer incidents are caused by vulnerabilities. In fact, more companies applied security patches regularly in 2004 (62.6%) than 2003 (47.2%).

Nevertheless, computer attack cannot be overlooked. There is rising variety of security threats which may affect or even destroy companies' computer systems suddenly. As a result, a well-established information security strategy should be deployed to protect companies' computer systems. However, many companies, especially SMEs, are reflexive. They apparently rely on experience or luck rather that proven information security management. The survey results reveal that the percentages of surveyed companies that had information security risk assessment and audit, information security policy and incident response procedures in place were still low in 2004, with only 11.6%, 18.1% and 22.6% respectively.

In fact, information security risk assessment is important to all companies, especially SMEs, to understand the risk and threats to the confidentiality, integrity and availability of company information and computer systems. From the results of the risk assessment, management can evaluate the costs and benefits of security countermeasures (including technology, people and process) to the companies and then decide on the most suitable one.

Therefore, companies have to keep on improving not only their security technologies but also security management. They should always update the latest trends and technologies on information security as well as stress on strategic planning and management on information security.

Summary Findings

Security technologies

- Ninety-six percent of the surveyed companies had deployed security technologies.
- "Anti-virus software" (90.9%), "Physical security" (65.5%), "Firewall" (65.4%) and Password (60.6%) were the four most commonly used security measures.
- The percentage of companies using "Firewall" increased significantly from 44.5% in 2003 to 65.4% in 2004.
- The awareness of information security increased significantly in 2004. The percentage of companies without any security measures dropped from 10.1% in 2003 to 3.6% in 2004.
- More companies in "Banking/Finance" (36.9%), "Manufacturing" (33.3%) and "Transport & Communication" (26.5%) sectors adopted Advanced security technologies.

Computer attacks

- Slightly over three-fifths of the interviewed companies (61.3%) had installed servers and/or web sites.
- Of these companies, 17.7% had suffered from computer attacks within the last 12 months.
- The total number of incidents recorded in the sample was 865 and the average number of attacks per victimized company was 2.7.
- A total of 3,464 PCs were affected and the average number of PCs affected per incident was 3.9.
- Small companies experienced a larger impact of computer attack.
- "Virus" (94.5%) was the most prevailing form of computer attack.
- The magnitude of financial losses further declined in 2004. The financial losses resulted from computer attacks decreased from HK$1.22 million in 2003 to HK$0.85 million in 2004, down by 30.1%.
- Slightly over two-fifths of the attacks were from overseas (42.9%).

Actions against computer attacks

- Most of the companies suffered from computer attacks in the last 12 months had patched the security holes (96%) after the attacks. Only 2.8% and 0.9% had reported to HKCERT and the police respectively.
- "Trivial, no need to report" (53.7%) was the major reason for not reporting to the police.

- The major reasons for not reporting to HKCERT were "Trivial, no need to report" (44.2%), "Unaware of HKCERT" (37.5%) and "Internal remedy is the best" (15.8%).

Security management

- The percentage of interviewed companies that had information security risk assessment and audit, information security policy and incident response procedures in place were still low in 2004, with only 11.6%, 18.1% and 22.6% respectively.
- Slightly more than three-fifths of the surveyed companies applied security patches regularly (62.6%).
- Close to two-fifths of the responded companies (37.4%) employed full-time or part-time staff to deal with information security issues.
- The share of annual IT expenditure on information security dropped in 2004. On average, only 3.1% of the annual IT expense was allocated to information security in 2004 as compared to 4.3% in 2003.
- Larger companies tend to have a higher spending ratio on information security.

Figures at a glance – 2000 to 2004

	2000	**2001**	**2002**	**2003**	**2004**
Total no. of incidents	1,510	1,387 *(-8.1%)*	1,095 *(-21.1%)*	943 *(-13.9%)*	865 *(-8.3%)*
Average no. of attacks per victimized company	2.6	3.5 *(+34.6%)*	3.4 *(-4%)*	2.4 (-29.4%)	2.7 *(+12.5%)*
Total no. of PCs affected	4,733	5,366 *(+13.4%)*	5,460 *(+1.8%)*	4,098 *(-24.9%)*	3,464 *(-15.5%)*
Average no. of PCs affected per incident	3.1	3.9 *(+25.8%)*	5 *(+28.2%)*	4.3 *(-14%)*	3.9 *(-9.3%)*
Total financial loss	HK$1.38M	HK$1.52M *(+10.8%)*	HK$1.84M *(+20.5%)*	HK$1.22M *(-33.5%)*	HK$0.85M *(-30.1%)*
Average financial loss per victimized company	HK$2,461	HK$3,888 *(+58%)*	HK$5,632 *(+44.9%)*	HK$3,116 *(-44.7%)*	HK$2,617 *(-16%)*