Information Security Survey 2003

December, 2003

Conducted by:

HKCERT

Technology Crime Division
Commercial Crime Bureau

Information Technology
Services Department
資訊科技署

ã 2003. The information contained in this document has been obtained from sources generally available to the public or released by responsible individuals in the subject companies but is not guaranteed as to accuracy or completeness. HKCERT, HKPF and ITSD will not be liable for errors, omissions or inadequacies in the information contained here or for interpretations thereof. The readers assume sole responsibility for selecting the information to achieve their own purposes.

Background

In view of the importance of understanding the information security status in Hong Kong, it is necessary to undertake an ongoing study to keep track of the extent of computer attacks, the level of information security awareness, technologies adoption, security strategy employed and information security expense in Hong Kong.

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 Information Technology Services Department (ITSD) of The Government of the Hong Kong Special Administrative Region (HKSAR).

This is the fourth time that such a study has been carried out. Three 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.

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 2002 survey was revised to address the specific objectives of the current study. The draft questionnaire was then commented by HKCERT, HKPF, ITSD 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 2003.

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.

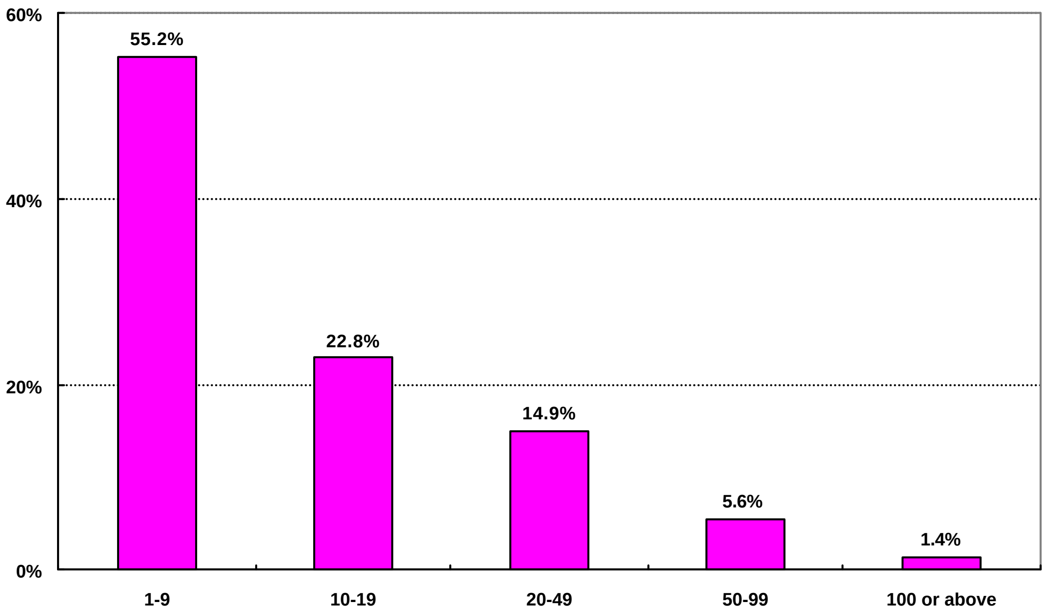
Quality control techniques included cross-checking of data integrity and random call-back to the sample units. Data cleaning and verification by scientific measures were also implemented throughout the fieldwork and data analysis stages.

Sample demographics

Staff size

Seventy eight percent of the surveyed companies were operating on a small scale, with 1-19 employees. One-fifth of them were medium-sized enterprises hiring 20-99 staff. The remaining 1.4% were large organizations having 100 employees or more (see Figure 1)

Figure 1: Sample distribution by staff size

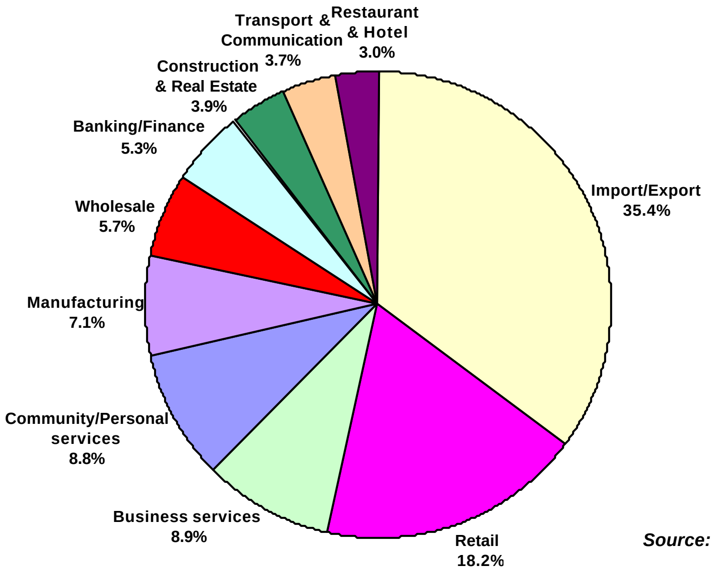


Source: HKCERT 2003

Industry sector

The distribution of the sample units by industry follows the spectrum of the population. Interviewed companies were concentrated in the "Import/Export" sector (35.4%), followed by the "Retail" sector (18.2%).

Figure 2: Sample distribution by industry sector



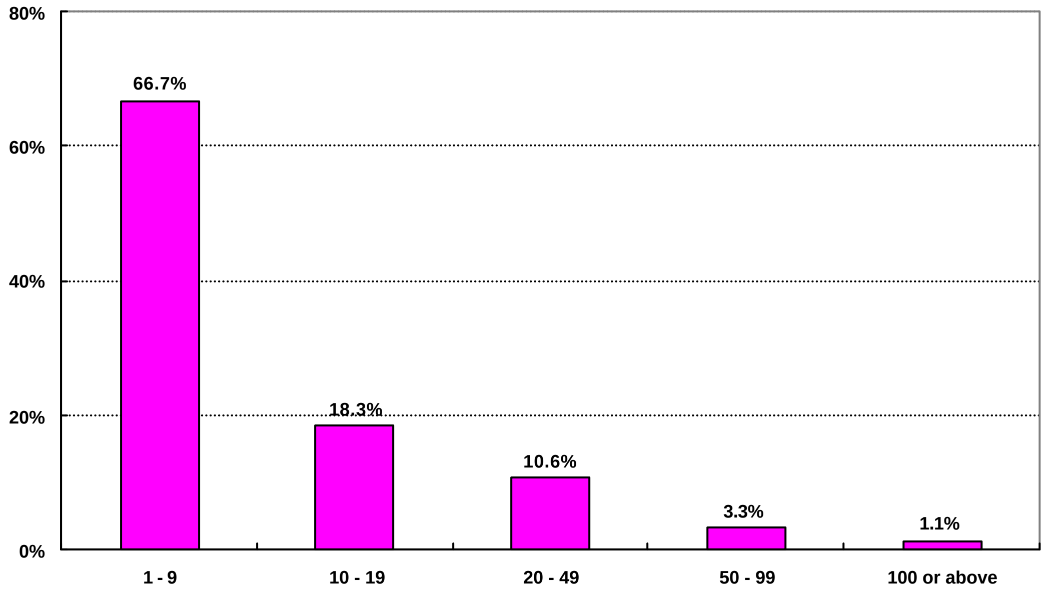
Source: HKCERT 2003

Major Findings

Number of PCs installed

The personal computer (PC) usage level skewed towards the low-end, largely explained by the dominance of small and medium-sized enterprises (SMEs) in the sample. Figure 3 illustrates that two-thirds of the surveyed companies had installed 1-9 PCs. Only 1.1% had installed 100 PCs or above.

Figure 3: Number of PCs installed



Source: HKCERT 2003

Security technology

Figure 4 shows that the majority of the surveyed companies (89.9%) had deployed various levels of security technologies to protect their computers and information. The four most popular security measures were "Anti-virus software" (81.2%), "Password" (53.1%), "Physical security" (44.5%) and "Firewall" (44.5%). However, still one-tenth of the surveyed companies did not use any security measures.

Compared with the data in previous studies, the use of "Firewall" increased significantly in 2003. An increasing number of companies begin to understand that basic security tools may not be sufficient to stop virus or other computer attacks. Therefore, more companies tend to install firewall to further protect their computer systems.

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

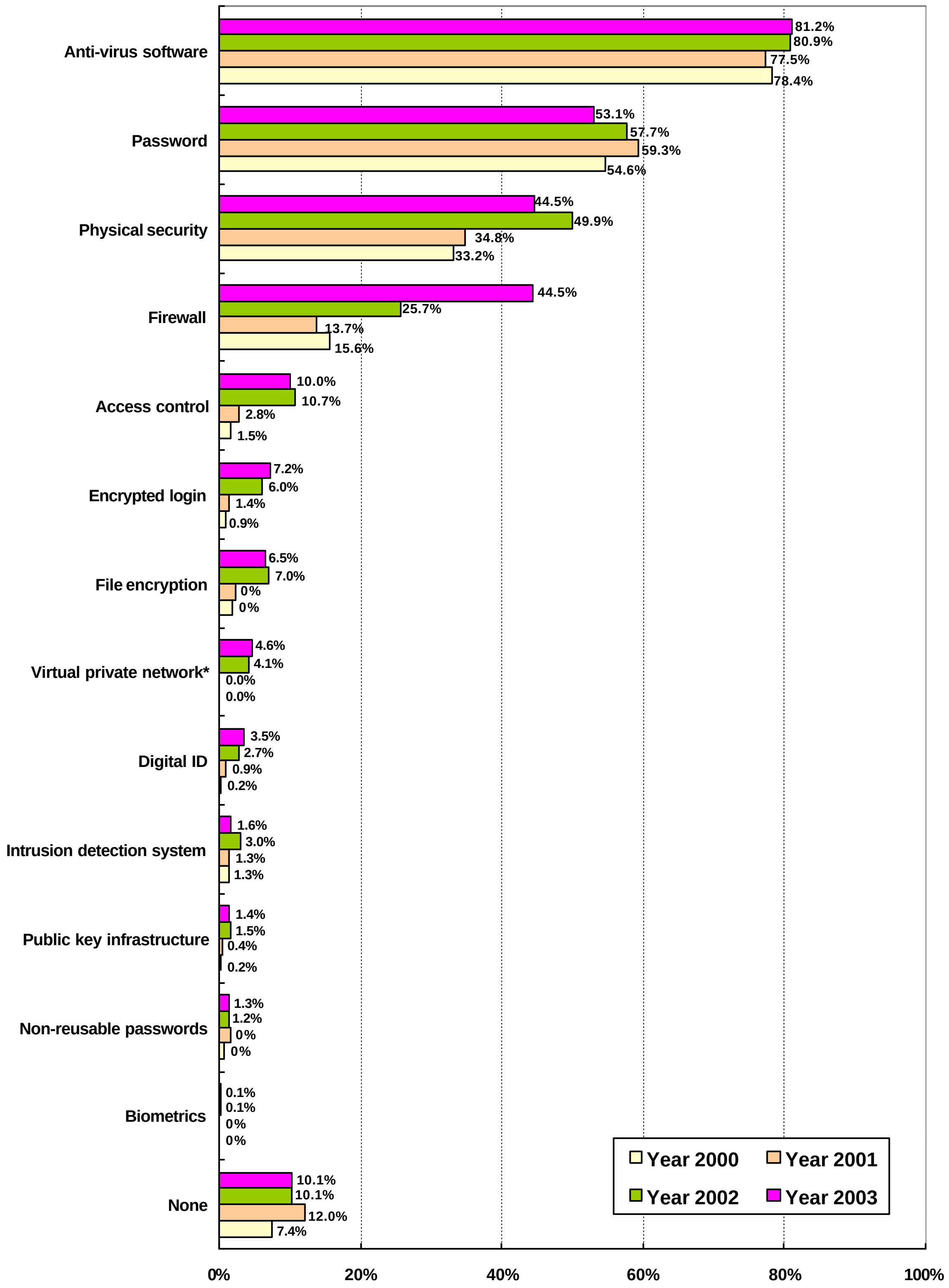
In 2003, each small firm adopted 2.3 security measures on average whereas the figure for medium companies was 3.9. These numbers were the same as the values in 2002.

On the other hand, the average number of security measures for large enterprises has increased remarkably from 4.9 in 2002 to 5.3 in 2003.

Table 1: Security technologies adopted by staff size (2002-2003)

	1-19		*20-99*		*100 or above*	
	2002	**2003**	**2002**	**2003**	**2002**	**2003**
Anti-virus software	78.6%	78.2%	89.6%	91.7%	94.1%	92.9%
Password	52.8%	46.6%	76.5%	76.3%	85.3%	76.2%
Physical security	45.8%	40.6%	65.2%	58.7%	76.5%	57.1%
Firewall	20.3%	38.5%	44.8%	64.3%	76.5%	85.7%
Access control	4.4%	4.4%	35.3%	28.2%	41.2%	57.1%
File encryption	3.2%	3.5%	21.3%	15.9%	32.4%	33.3%
Encrypted login	2.9%	3.7%	18%	19.3%	23.5%	28.6%
Virtual Private Network	1.7%	1.2%	12.8%	14.7%	29.4%	40.5%
Intrusion detection system	1.5%	1.0%	8.5%	3.6%	8.8%	7.1%
Digital ID	1.5%	1.7%	7.4%	9.1%	5.9%	19.0%
Public Key Infrastructure	0.8%	0.7%	4.2%	3.4%	2.9%	9.5%
Non-reusable passwords	0.5%	0.3%	3.8%	3.9%	11.8%	16.7%
Biometrics	0.1%	0%	0.3%	0.5%	0%	2.4%
Others	0.1%	0%	0.3%	0%	0%	0%
None	11.6%	12.1%	4.2%	3.1%	5.9%	2.4%
Total	***225.6%***	***232.5%***	***392.2%***	***392.7%***	***494.1%***	***528.6%***
Average number of security measures per company	***2.3***	***2.3***	***3.9***	***3.9***	***4.9***	***5.3***

Figure 4: Security technologies adopted (2000-2003)



**Virtual private network was not included in 2001 & 2002 studies*

Source: HKCERT 2003

Security level

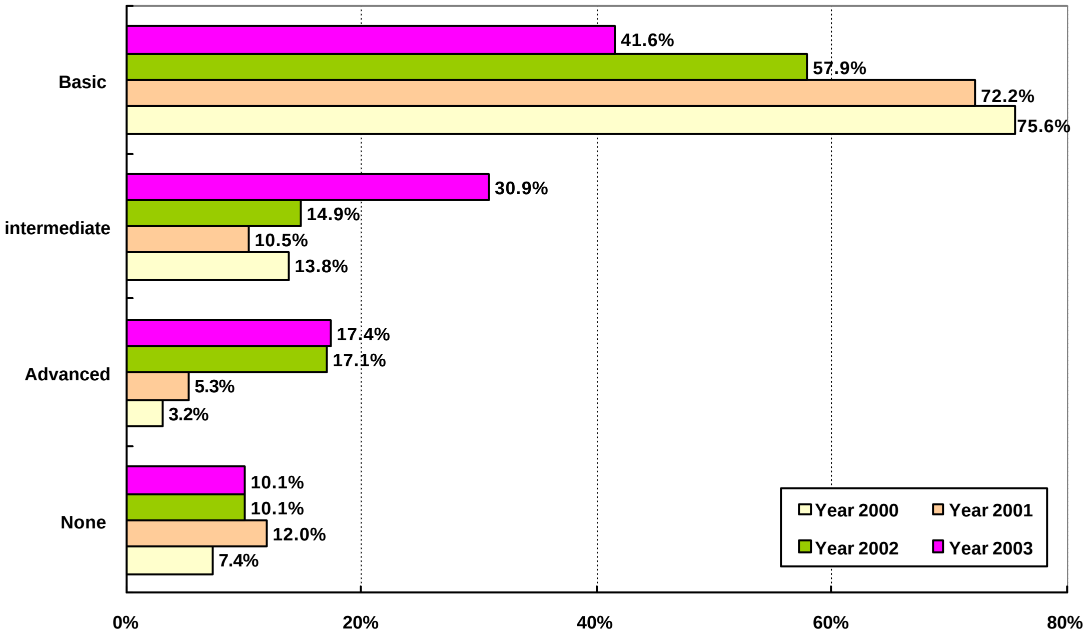
For further analytical purposes, we have defined four security levels, namely None, Basic, Intermediate and Advanced. Detailed classifications are listed in Table 2.

Table 2: Classification of security technologies

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

Survey results reveal that increasingly more companies are using higher levels of security measures to safeguard against computer attacks. The current survey shows that nearly half of the interviewed companies belonged either to the Intermediate or Advanced security level while the percentage in 2002 was only 32%.

Figure 5: Security level (2000-2003)



Source: HKCERT 2003

The security level correlates with the staff size. Among the small companies surveyed, the use of Basic security measures was dominant (47%) whereas 71.4% of the large enterprises utilized Advanced security technologies to prevent security breaches in 2003 (see Table 3).

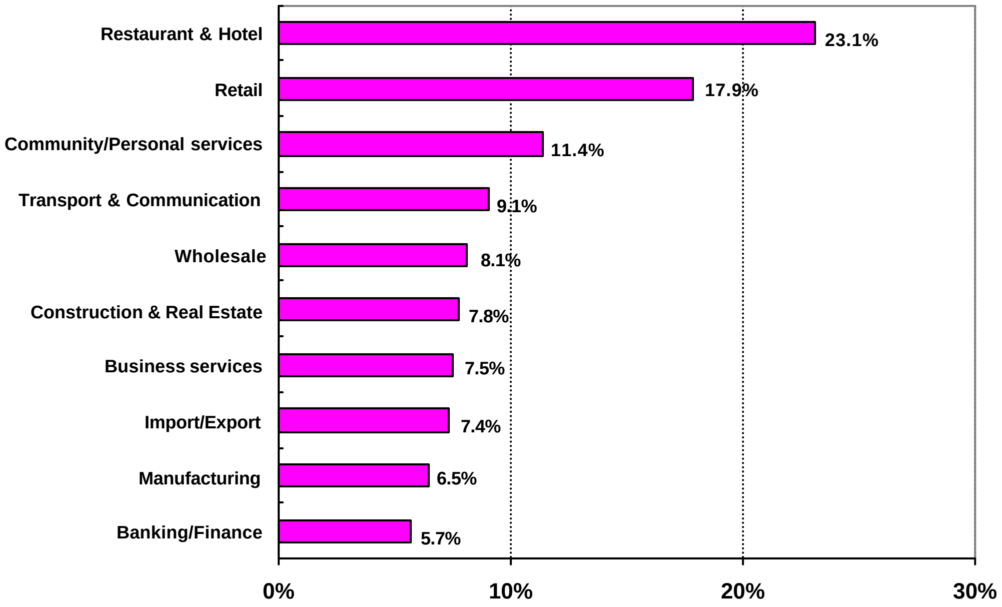
Although the overall security level has improved in 2003, a large portion of SMEs are still using lower levels of security technologies. This is an area of concern as many of these companies are less technology competent. They are more vulnerable to computer attacks and subsequent damages.

Table 3: Security level by staff size (2002-2003)

	1-19		*20-99*		*100 or above*	
	2002	**2003**	**2002**	**2003**	**2002**	**2003**
None	11.6%	12.1%	4.2%	3.1%	5.9%	2.4%
Basic	64.9%	47%	31.7%	23.5%	11.8%	9.5%
Intermediate	15.3%	32.1%	13.7%	27.2%	8.8%	16.7%
Advanced	8.2%	8.8%	50.5%	46.2%	73.5%	71.4%
Total	***100%***	***100%***	***100%***	***100%***	***100%***	***100%***

More companies in “Restaurant & Hotel” (23.1%), “Retail” (17.9%) and “Community/Personal Services” (11.4%) sectors did not use any security technologies.

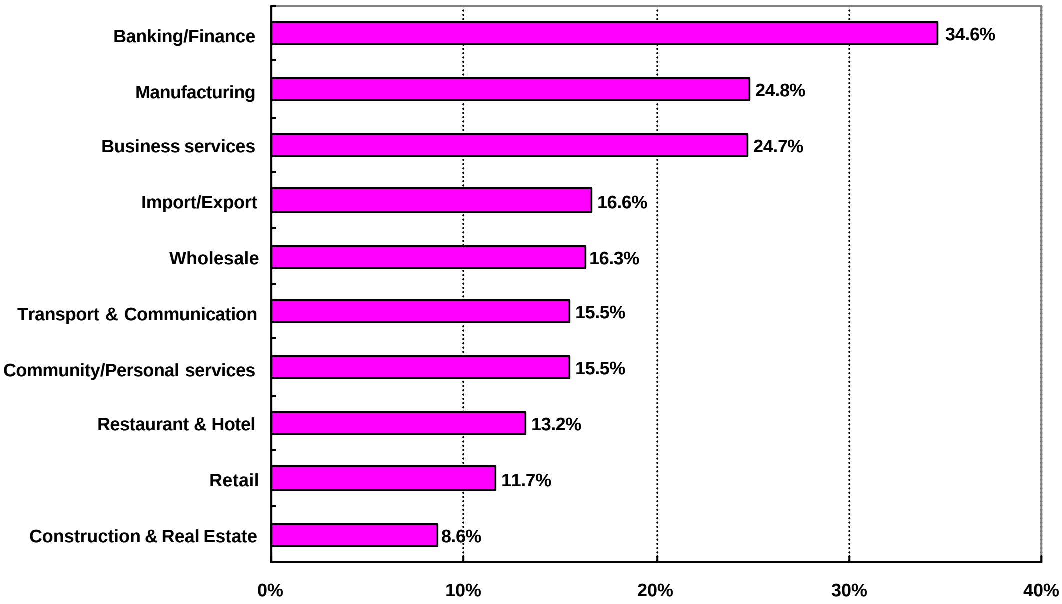
Figure 6: No security technologies in place by industry sector



Source: HKCERT 2003

On the other hand, “Banking/Finance”, “Manufacturing” and “Business services” sectors were better prepared for the attacks, with 34.6%, 24.8% and 24.7% adopting Advanced security technologies correspondingly (see Figure 7).

Figure 7: Advanced security level by industry sector



Source: HKCERT 2003

Computer attacks

The current study shows that over half of the interviewed companies (56.2%) had installed servers and/or web sites. Of these companies, 23.3% (392 out of 1,685 companies) had experienced computer attacks within the last 12 months. Fifty six percent of the victimized companies reported 2-4 incidents and one-third mentioned once.

The total number of incidents recorded in the sample decreased from 1,095 incidents in 2002 to 943 incidents in 2003, down by 13.9%. In addition, the average number of attacks per victimized company dropped from 3.4 in 2002 to 2.4 in 2003 (see Table 4).

The decrease in number of computer attacks can be attributed to the improved security technologies deployed.

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

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

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 dropped in 2003 after reaching a peak in 2002.

A total of 4,098 PCs were affected in 2003, down by 24.9% from 2002. In addition, the average number of PCs affected per incident dropped from 5 in 2002 to 4.3 in 2003.

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

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

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 (2000-2003)

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

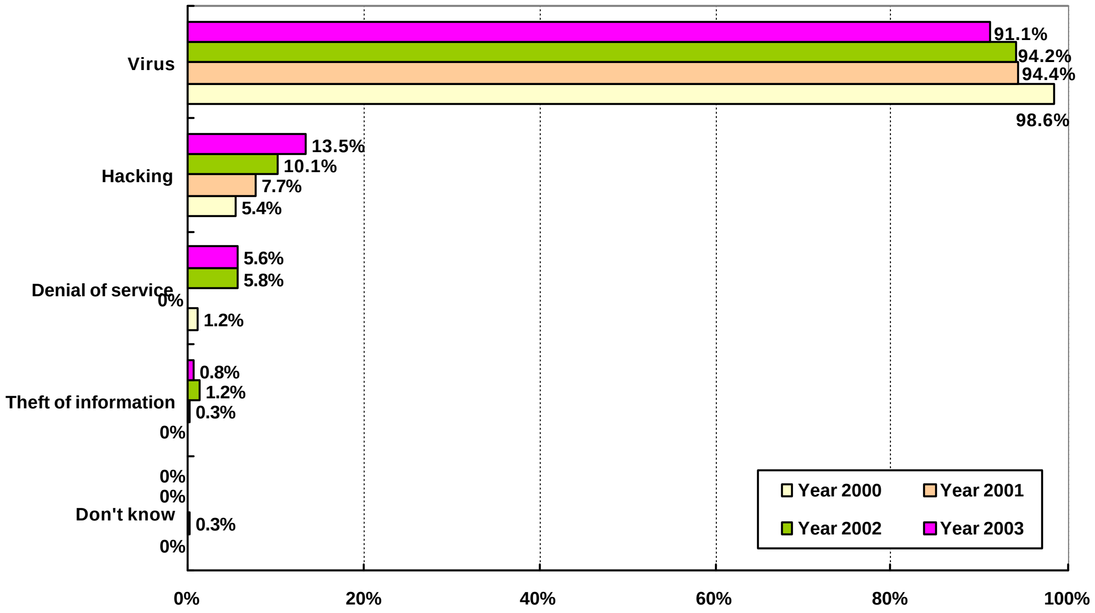
Table 6 shows that the average number of PCs affected per incident increases with company size. However, in general, the numbers decreased within all size groups in 2003 as compared to the figures in 2002.

In terms of the impact per computer attack, it is found that small companies suffered a much larger impact (0.43) than medium-sized (0.23) or large companies (0.31). Overall speaking, the impacts were reduced when compared with the findings in 2002.

Tables 5 and 6 present an encouraging signal as the extend and impact of computer attacks had diminished in 2003.

Regarding the types of computer attack, the distribution pattern remained approximately the same as in previous studies. Computer virus (91.1%) is still the most prevailing form of computer attack, followed by hacking (13.5%) and denial of service (5.6%).

Figure 8: Types of computer attack (2000-2003)



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

Source: HKCERT 2003

The magnitude of financial loss shrank in 2003. In the current study, a sum of HK$1.22 million was recorded among those companies that suffered from computer attacks, down by 33.5% from 2002 (see Table 7). This is a positive sign in that companies are paying more efforts to minimize the impact of the attacks and take quicker actions to handle the attacks once they are discovered.

Virus remained the dominant type of attack. It accounted for 67.1% of the monetary loss, equivalent to a sum of HK$0.82 million. The financial losses due to hacking, denial of service and theft of information were HK$0.29 million, HK$32,850 and HK$83,000 respectively.

In this survey, 32.6% of respondents reported that the incidents had resulted in financial losses. This ratio has declined from 54% in 2002 (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 7: Financial losses by type of computer attack within the last 12 months (2000-2003)

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

Table 8: No. of incidents by type of computer attack within the last 12 months (2000-2003)

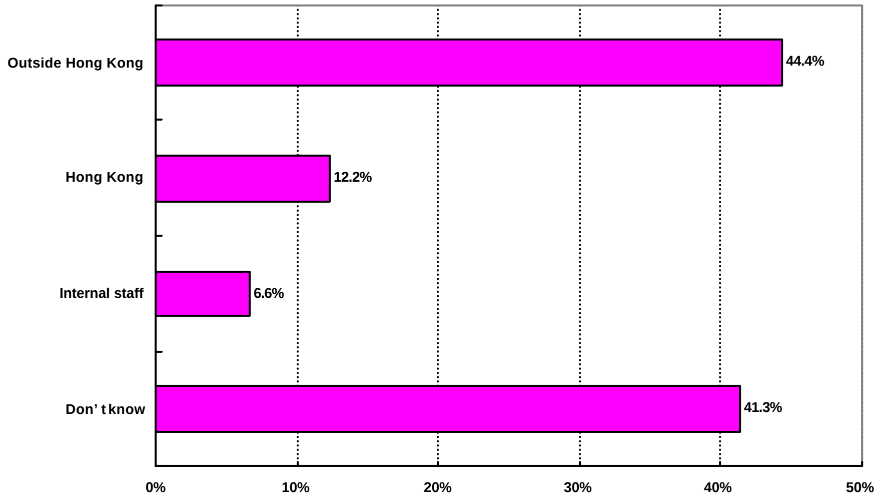
	No. of incidents			
Type of computer attack	**2000**	**2001**	**2002**	**2003**
Hacking	30	30	33	53
Denial of service	7	0	19	22
Virus	551	370	307	357
Theft of information	0	1	4	3
Total	***588***	***401***	***363***	***435***
% of incidents reported financial loss	***13.3%***	***37.4%***	***54%***	***32.6%***

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 44.4% of the attacks were from overseas while 12.2% were from Hong Kong.

Still, a lot of respondents (41.3%) did not know the origin of the attacks. As the attacks can strike 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 = 392 companies suffered from computer attacks in the last 12 months

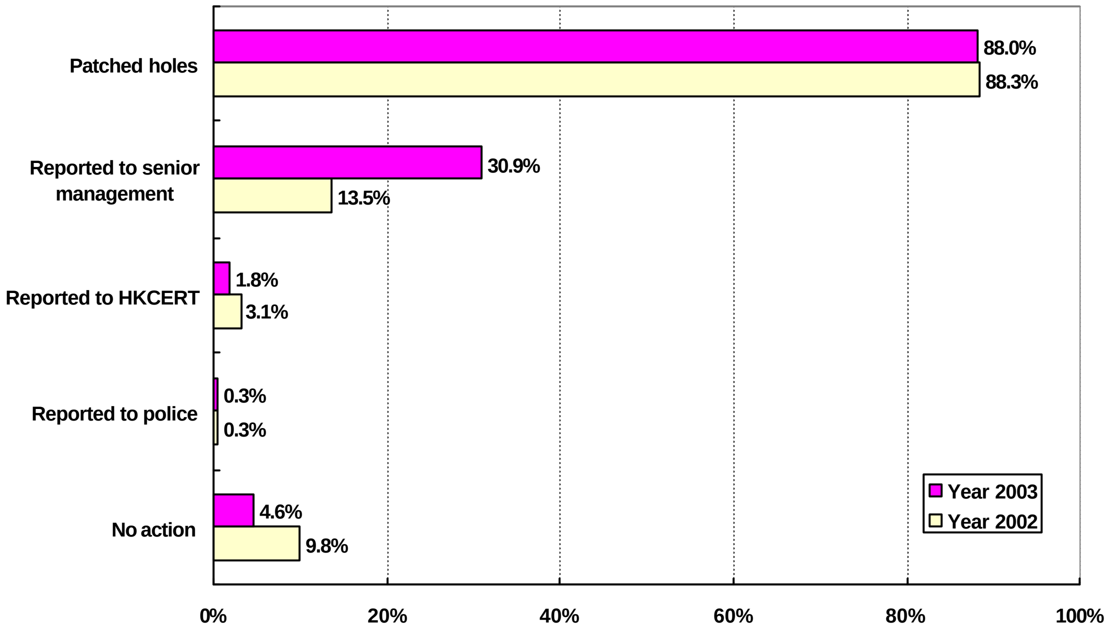
Source: HKCERT 2003

Actions against computer attacks

When asked how to deal with the computer attacks, most of the respondents (88%) replied that they would patch the security holes while 30.9% would report to senior management.

Only a few chose to report to HKCERT (1.8%) or the police (0.3%). Even worse, 4.6% expressed that they did not take any actions against computer attacks.

Figure 10: Actions against computer attacks (2002-2003)

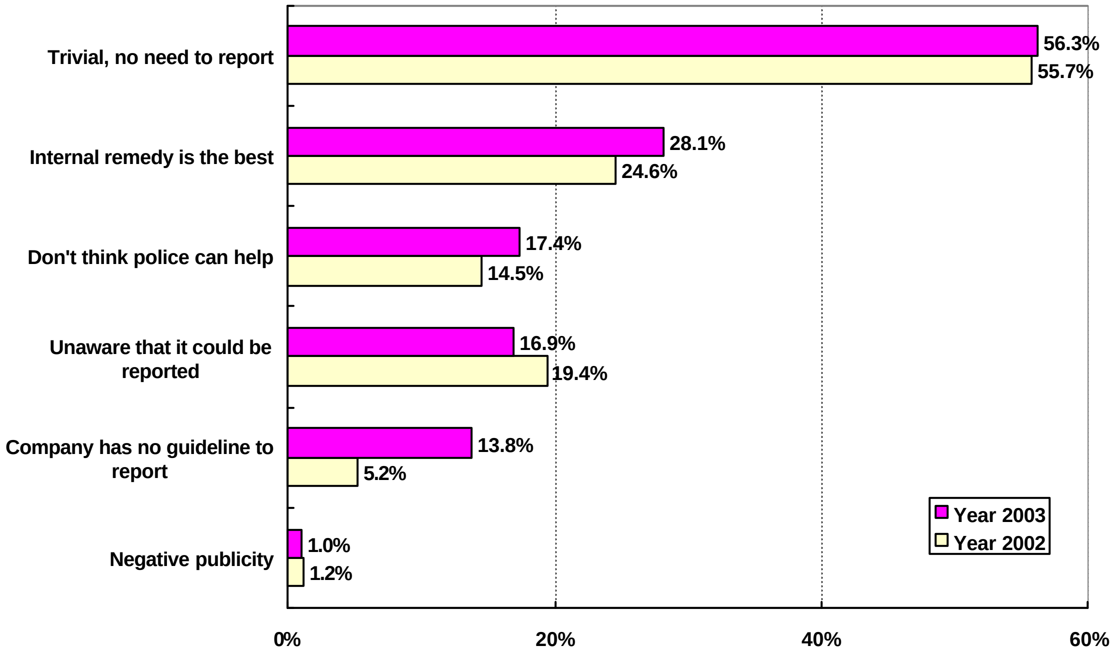


n = companies suffered from computer attacks in the last 12 months

Source: HKCERT 2003

The key reason for not reporting to the police was found to be "Trivial, no need to report" (56.3%). "Internal remedy is the best" (28.1%) was another more common explanation.

Figure 11: Reasons for not reporting to police (2002-2003)



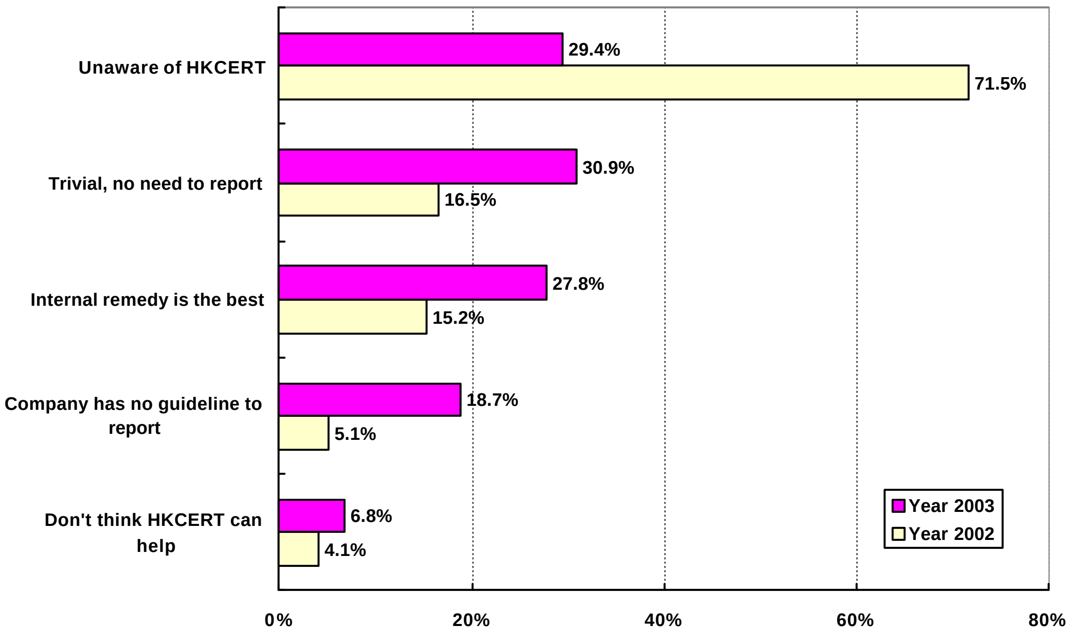
n = companies who had not reported to police after computer attacks

Source: HKCERT 2003

Respondents did not report to HKCERT mainly because "Trivial, no need to report" (30.9%), "Unaware of HKCERT" (29.4%) and "Internal remedy is the best" (27.8%) (see Figure 12).

When compared with the figure in 2002, the percentage of "Unaware of HKCERT" as the reason for not reporting to HKCERT was greatly reduced in 2003.

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



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

Source: HKCERT 2003

Security management

Security management is used in this survey to cover four aspects, including information security risk assessment and audit, information security policy, incident response procedures and regularly applying security patches.

Overall speaking, many companies have not taken any initiatives in preventing or tackling computer breaches. The percentages of surveyed companies that had information security risk assessment and audit, information security policy and incident response procedures in place were only 12.5%, 17.3% and 26.5% accordingly. Notwithstanding that, over half of the companies applied security patches regularly (53.1%) to safeguard their computer systems.

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

Table 9: Security management in place

Staff size	***Information security risk assessment and audit***	***Information security policy***	***Incident response procedures***	***Regularly applying security patches***
1-19	8.3%	11%	20.5%	47.2%
20-99	25.3%	38.6%	46.2%	73.3%
100 or above	57.1%	57.1%	69.0%	85.7%
All companies	***12.5%***	***17.3%***	***26.5%***	***53.1%***

The percentage of companies that had already implemented information security policy increased from 14.2% in 2002 to 17.3% in 2003. Table 10 and 11 compare the implementation rate of information security policy in 2002 and 2003 by staff size and by industry sector respectively.

Table 10: Implementation of information security policy by staff size (2002-2003)

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

Table 11: Implementation of information security policy by industry sector (2002-2003)

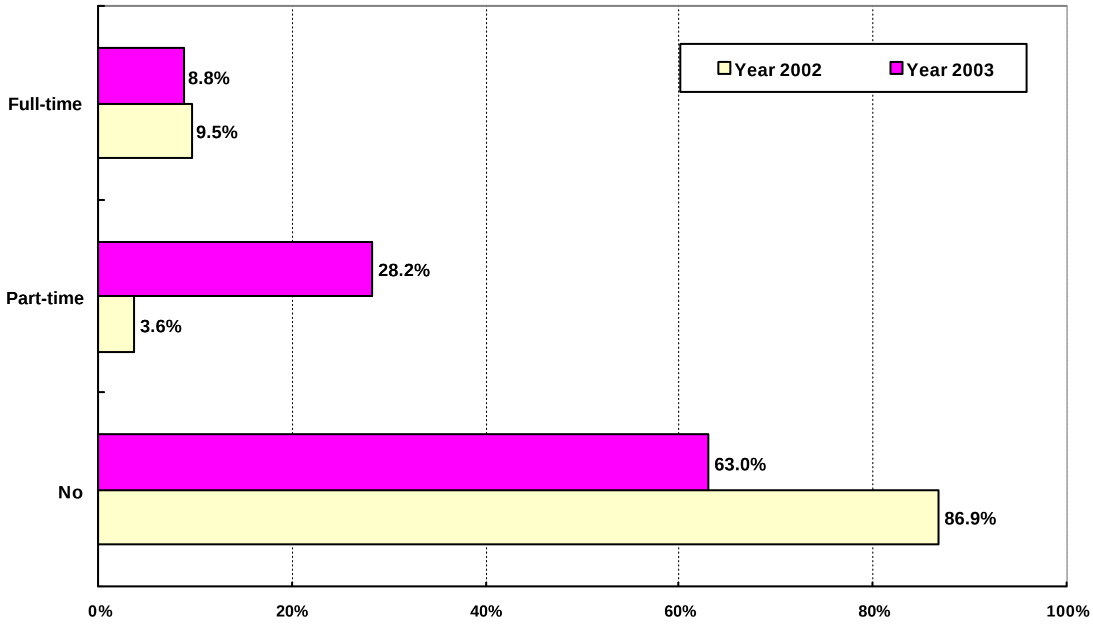
Industry sector	2002	2003
Banking/Finance	30.4%	30.8%
Restaurant & Hotel	20.6%	17.6%
Manufacturing	18.2%	22.4%
Business services	16.3%	22.8%
Community/Personal services	14.2%	19.3%
Import/Export	13.4%	16.7%
Transport & Communication	11.9%	20.0%
Retail	10.6%	12.3%
Construction & Real Estate	9.7%	6.9%
Wholesale	7.7%	12.2%
All sectors	**14.2%**	**17.3%**

Information security staff

Close to two-fifths of the surveyed companies (37%) employed full-time or part-time staff to deal with information security issues (see Figure 13). In particular, the percentage of companies with part-time information security staff has increased significantly from 3.6% in 2002 to 28.2% in 2003.

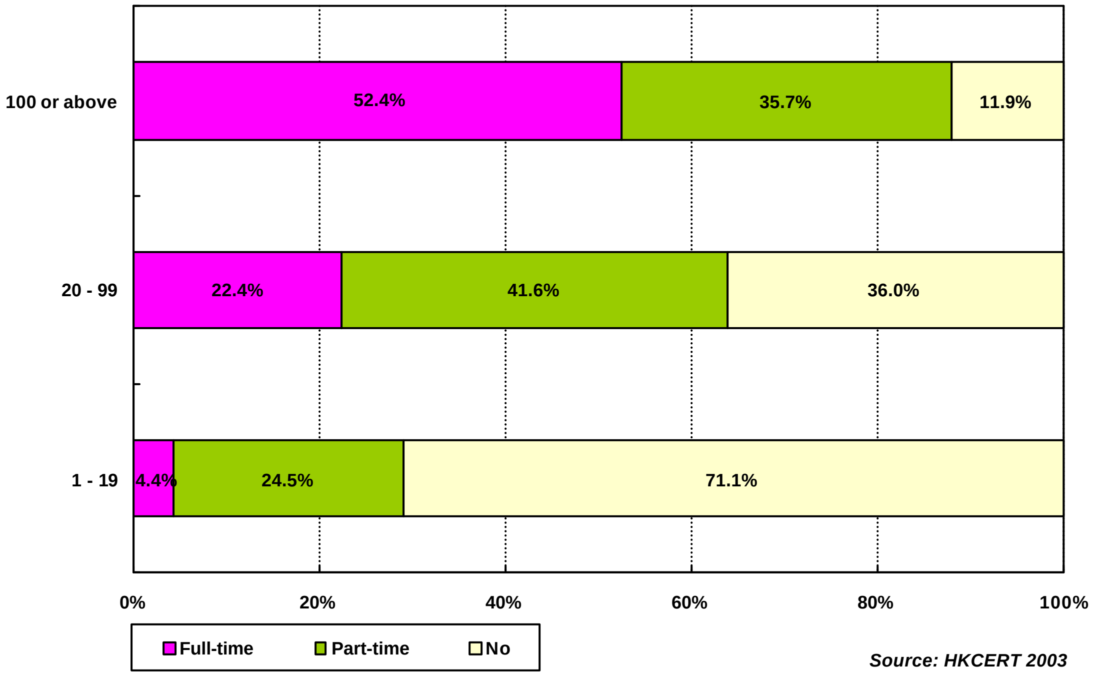
Large companies are more inclined to employ delegate persons to look after their company systems to prevent computer attacks. Figure 14 shows that 88.1% of the large companies had full-time or part-time staff responsible for information security whereas only 28.9% of small enterprises hired information security staff.

Figure 13: In-house information security staff (2002-2003)



Source: HKCERT 2003

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



Source: HKCERT 2003

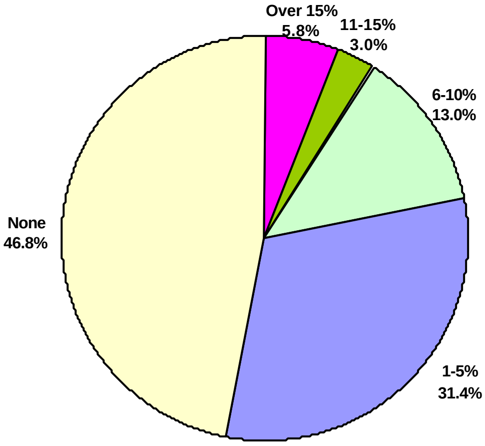
Information security expense

Close to half of the surveyed companies expressed that no expenses on information security were incurred in the last 12 months (see Figure 15). On the other hand, 31.4% of sample units stated that 1-5% of their annual IT expenditure were spent on information security. Only 5.8% had spent over 15% of their annual IT expenses on information security.

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

- No information security technologies had been deployed.
- Information spending could not be separated from the IT spending.
- The spending on information security expense was not incurred on 2003.
- Obtaining free anti-virus software from the public.

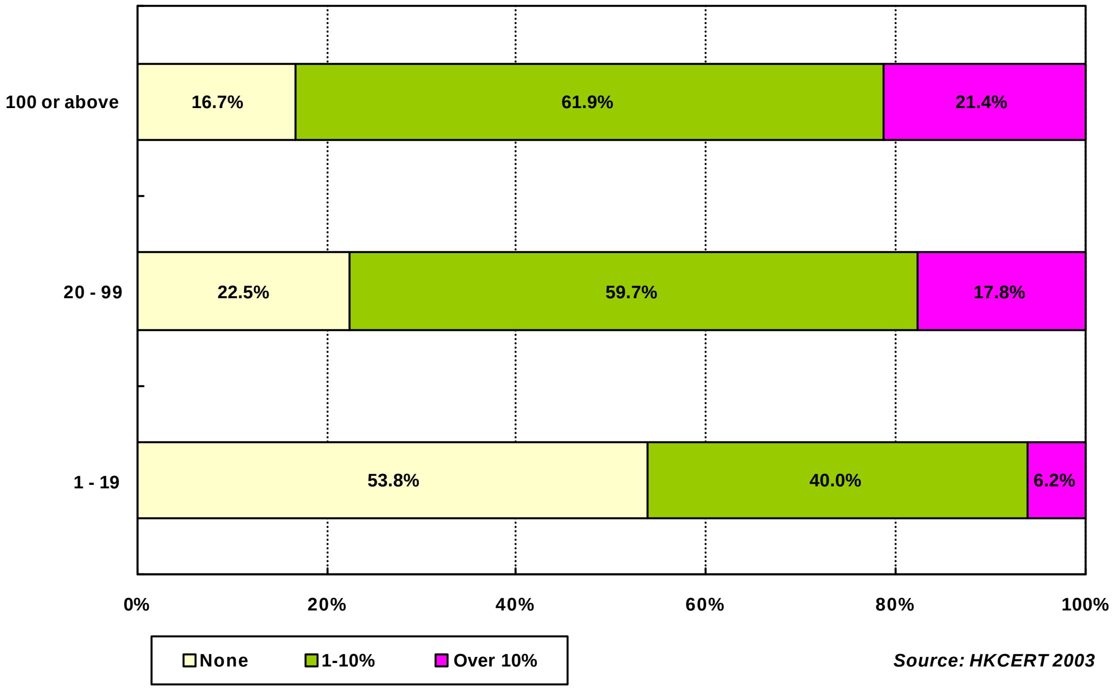
Figure 15: Information security expense



Source: HKCERT 2003

The percentage of IT spending allocated to information security varies 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



Source: HKCERT 2003

On average, company spent 4.3% of its IT expenses on information security within the last 12 months (see Table 12). The ratio increased with company size.

Table 12: Average percentage of annual IT expenses on information security by staff size

Staff size	**Spending on information security**
1-19	3.4%
20-99	7.3%
100 or above	8.8%
Total	**4.3%**

Summary Findings

Security technologies

- Ninety percent of the surveyed companies had deployed security technologies.
- "Anti-virus software" (81.2%), "Password" (53.1%), "Physical security" (44.5%) and "Firewall" (44.5%) were the four most common security measures.
- The percentage of companies using "Firewall" increased significantly from 25.7% in 2002 to 44.5% in 2003.
- The overall security level had been improved over the past three years. However, the security level amongst small companies was still low with 12.1% having no security technologies in place and 47% belonging to the Basic level.
- More companies in "Banking/Finance" (34.6%), "Manufacturing" (24.8%) and "Business services" (24.7%) sectors adopted Advanced security technologies.

Computer attacks

- Over half of the respondents (56.2%) reported that their companies had servers and/or web sites.
- Of these companies, 23.3% had suffered from computer attacks within the last 12 months.
- The total number of incidents recorded in the sample was 943 and the average number of attacks per victimized company was 2.4.
- A total of 4,098 PCs were affected and the average number of PCs affected per incident was 4.3.
- Small companies experienced a larger impact of computer attack, with a higher percentage of PCs being affected.
- "Virus" (91.1%) was the major form of computer attack in 2003.
- The financial loss resulted from computer attacks decreased from HK$1.84 million in 2002 to HK$1.22 million in 2003, down by 33.5%.
- Over two-fifths of the attacks were from overseas (44.4%).

Actions against computer attacks

- Most of the companies suffered from computer attacks in the last 12 months had patched the security holes (88%) after the attacks. Only 1.8% and 0.3% had reported to HKCERT and the police respectively.
- "Trivial, no need to report" (56.3%) and "Internal remedy is the best" (28.1%) were the two main reasons for not reporting to the police.

- The major reasons for not reporting to HKCERT were “Trivial, no need to report” (30.9%), “Unaware of HKCERT” (29.4%) and “Internal remedy is the best” (27.8%).

Security management

- The percentage of surveyed companies that had information security risk assessment and audit, information security policy and incident response procedures in place were 12.5%, 17.3% and 26.5% respectively.
- Slightly over half of the companies applied security patches regularly (53.1%).
- Thirty seven percent of the interviewed companies employed full-time or part-time staff to deal with information security issues.
- On average, company spent 4.3% of its IT expenses on information security in 2003.

Figures at a glance – 2000 to 2003

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