Information Security Survey 2002

December, 2002

Conducted by:

HKCERT

Technology Crime Division
Commercial Crime Bureau

ITS
Information Technology
Services Department
資訊科技署

© 2002. 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 order to keep track of the extent of computer attacks, the level of information security awareness and the protection strategy employed in Hong Kong, an ongoing study program is important so that we can take the appropriate actions.

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 of The Government of the Hong Kong Special Administrative Region (ITSD).

This is the third time that such kind of study is carried out. Two previous studies had been conducted in October 2001 and 2000. This report not only presents detailed findings from the current study but also compares the results with the previous studies.

Objectives

This study aims to investigate the information security status in Hong Kong in 2002. The objectives are to:

- Serve as an update of the previous studies conducted in 2001 and 2000.
- Find out the latest security technologies adopted by companies in Hong Kong.
- Investigate the types of computer attacks and their impacts.
- Understand the actions that companies have taken to deal with the attacks.
- Examine the implementation of information security policy and the availability of in-house information security staff.

Methodology

Sampling frame and criteria

Target sample units were registered companies in Hong Kong that utilized computers. Respondents were either 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 the Census & Statistics Department. Proportional sampling was adopted to ensure the distribution of the sample units by industry sector and staff size followed a similar pattern as that of the population.

Survey method

The previous questionnaire used in the 2001 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 information and a total of 3,000 questionnaires were completed between August and September 2002.

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.

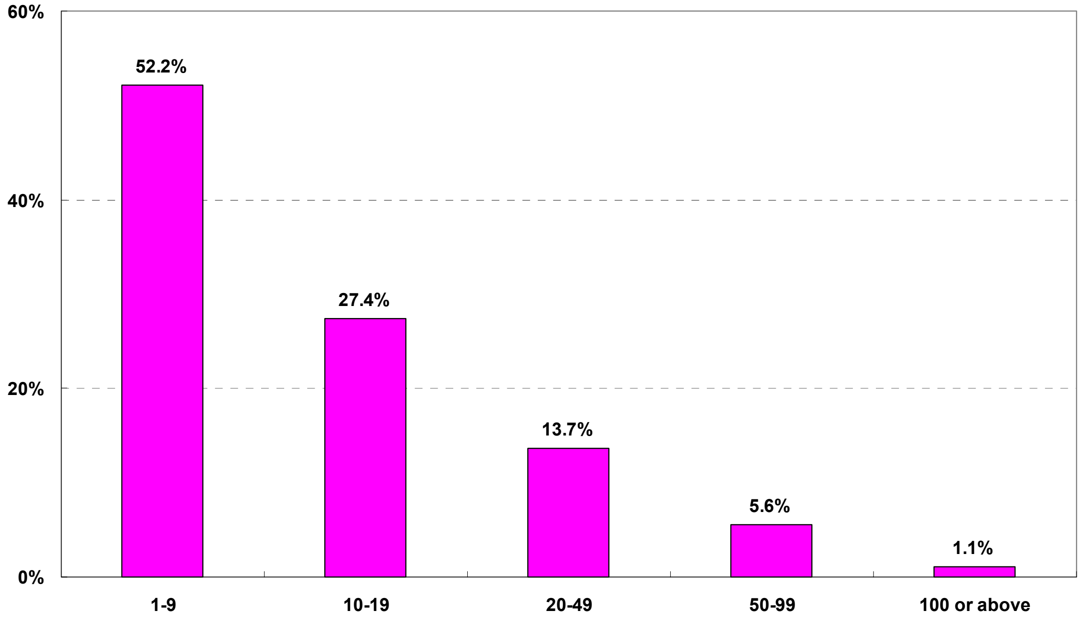
Quality control techniques included cross-checking of data integrity and random call-back to sample units. Data cleaning and verification by scientific measures were also implemented throughout the fieldwork and data analysis stages.

Sample demographics

Staff size

Four-fifths of the companies surveyed were small entities, with an employment size of 1-19. Almost twenty per cent (19.3%) were medium-sized companies employing 20-99 staff. The remaining 1.1% were large enterprises having 100 employees or more (see Figure 1).

Figure 1: Sample distribution by staff size

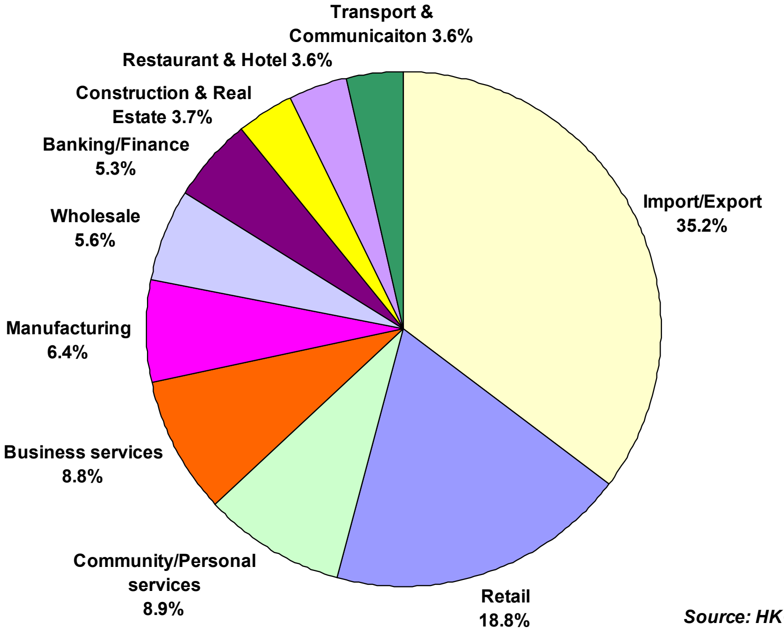


Source: HKCERT 2002

Industry sector

As illustrated in Figure 2, slightly more than one-third of the sample units (35.2%) came from the Import/Export sector, followed by the Retail sector (18.8%). The distribution of the sample reflects the pattern seen in the community as a whole.

Figure 2: Sample distribution by industry sector



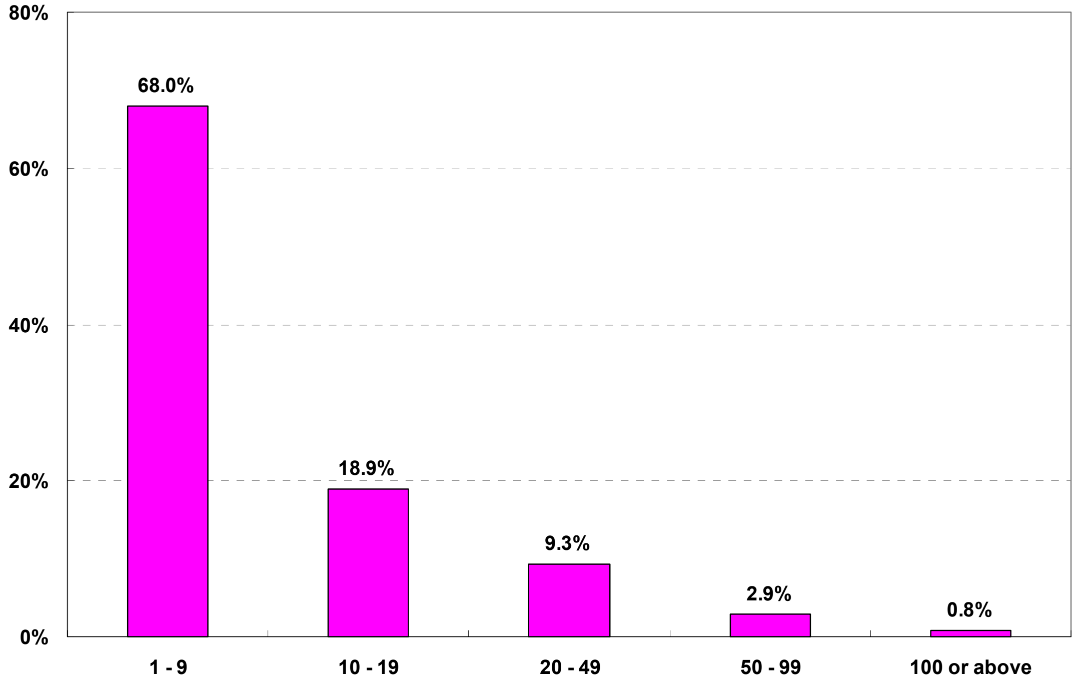
Source: HKCERT 2002

Major Findings

Number of PCs installed

The personal computer (PC) usage level appears to be skewed towards the low-end, largely explained by the dominance of small to medium-sized enterprises in the sample. As shown in Figure 3, 68% of the surveyed companies had an installation base of 1-9 PCs. Only 0.8% installed more than 100 PCs.

Figure 3: Number of PCs installed



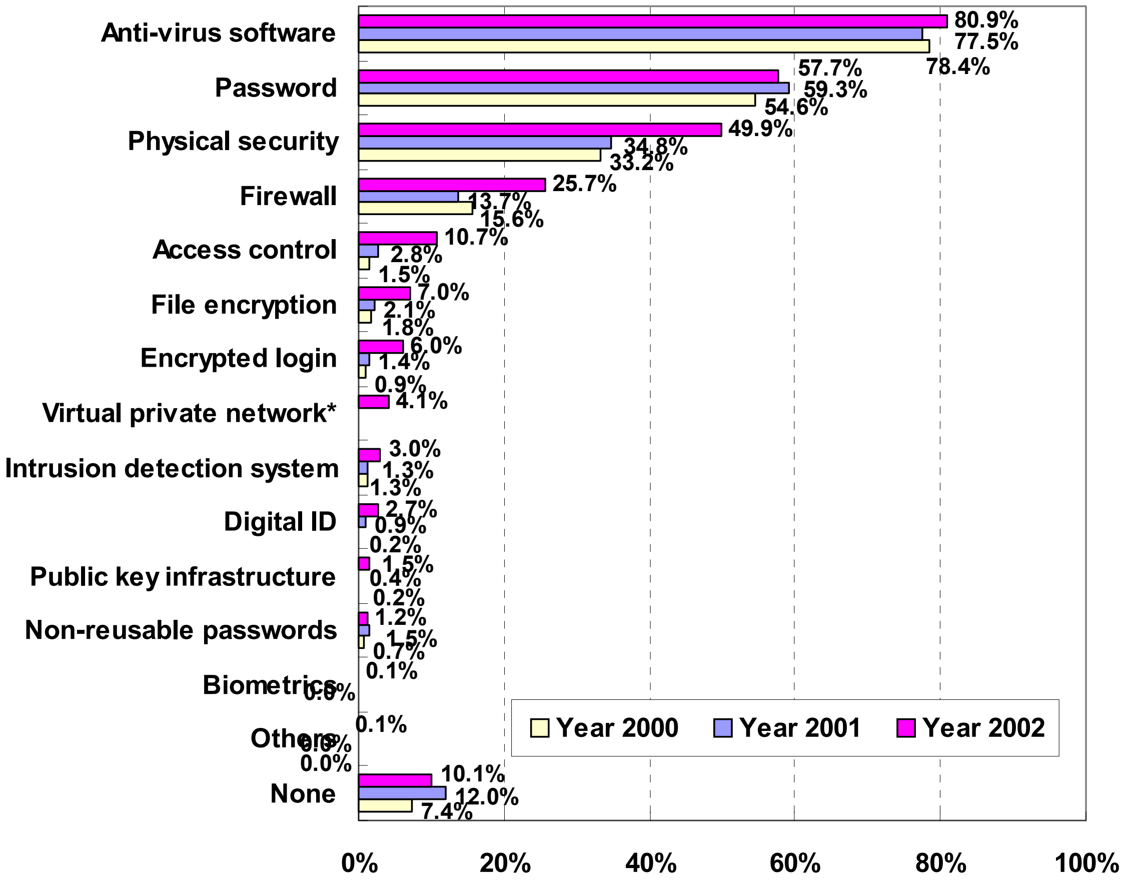
Source: HKCERT 2002

Security technology

Ninety per cent of the interviewed companies had adopted security technologies to protect their company information. The three most popular measures were "Anti-virus software" (80.9%), "Password" (57.7%) and "Physical security" (49.9%).

Overall speaking, the adoption rate of different kinds of security technologies has increased over the past two years. However, there are still 10.1% of the surveyed companies not using any security technologies.

Figure 4: Security technologies adopted (2000-2002)



***Virtual private network was not included in the previous studies**

Source: HKCERT 2002

Table 1 presents the security technologies adopted by staff size. On average, each small enterprise adopts 2.1 security measures in 2002. For medium and large companies, the average number of security measures is 3.9 and 4.9 respectively.

Regarding the security technology, it is found that the use of Password and Non-reusable passwords is decreasing notably in medium and large companies while the adoption of Firewall increases significantly in all kinds of companies.

Table 1: Security technologies adopted by staff size (2001-2002)

	1-19		***20-99***		***100 or above***	
	2001	**2002**	**2001**	**2002**	**2001**	**2002**
Anti-virus software	73.9%	78.6%	91.6%	89.6%	93.1%	94.1%
Password	53.4%	52.8%	82.3%	76.5%	93.1%	85.3%
Physical security	29.2%	45.8%	56.2%	65.2%	79.3%	76.5%
Firewall	8.1%	20.3%	35.2%	44.8%	55.2%	76.5%
Access control	0.2%	4.4%	11.4%	35.3%	44.8%	41.2%
File encryption	0.1%	3.2%	8.9%	21.3%	37.9%	32.4%
Encrypted login	0%	2.9%	6.5%	18%	13.8%	23.5%
Virtual Private Network[1]	-	1.7%	-	12.8%	-	29.4%
Intrusion detection system	0%	1.5%	6.1%	8.5%	13.8%	8.8%
Digital ID	0.1%	1.5%	3.7%	7.4%	10.3%	5.9%
Public Key Infrastructure	0%	0.8%	1.8%	4.2%	3.4%	2.9%
Non-reusable passwords	0%	0.5%	6.5%	3.8%	24.1%	11.8%
Biometrics	0%	0.1%	0%	0.3%	0%	0%
Others	0%	0.1%	0%	0.3%	0%	0%
None	14.3%	11.6%	3.2%	4.2%	0%	5.9%
Total	179.3%	225.6%	313.4%	392.2%	468.8%	494.1%
Average number of security measures per company	1.7	2.1	3.1	3.9	4.7	4.9

[1] Virtual Private Network was not included in the previous studies

Security level

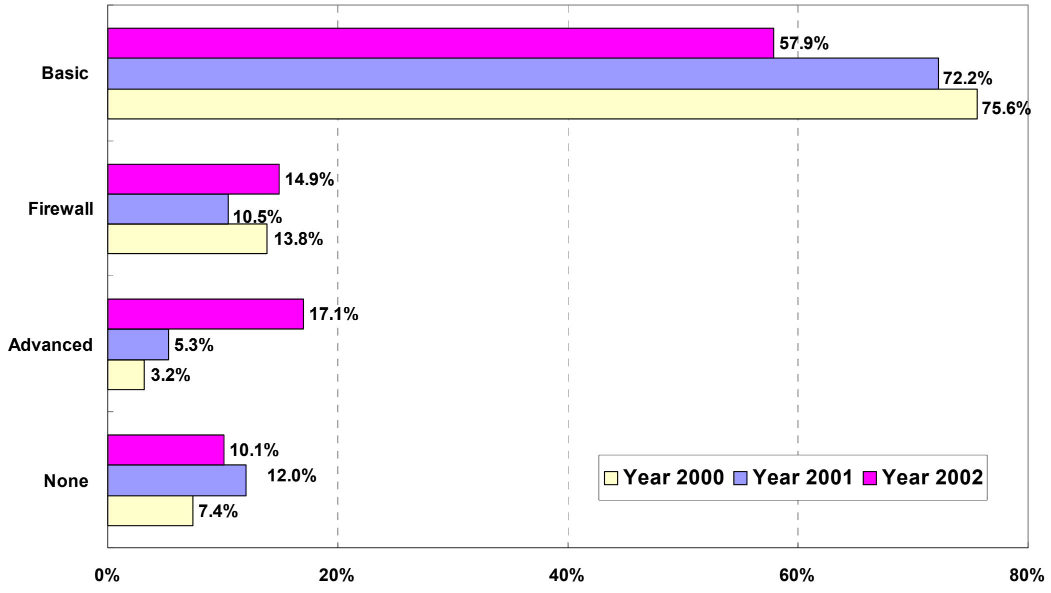
For further analysis purpose, all security technologies listed in this survey were classified into four levels, namely None, Basic, Firewall and Advanced. Detailed explanations are listed in Table 2.

Table 2: Classification of security technologies

Security Level	***Types of security technology adopted***
None	No use
Basic	Anti-virus software/Password/Physical security only
Firewall	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 there is a significant increase in the number of companies with higher security level. The current survey showed that 17.1% and 14.9% of interviewed companies belonged to the Advanced and Firewall levels respectively while only 5.3% employed Advanced security technologies and 10.5% deployed Firewall in 2001. This improvement is encouraging and it reflects that more companies recognize the importance of information security.

Figure 5: Security level (2000-2002)



Source: HKCERT 2002

The security level correlates with the staff size. Among the small companies surveyed, the use of Basic security measures was dominant (64.9%) whereas nearly three-quarters of the large enterprises utilized Advanced security technologies to prevent security breaches in 2002 (see Table 3).

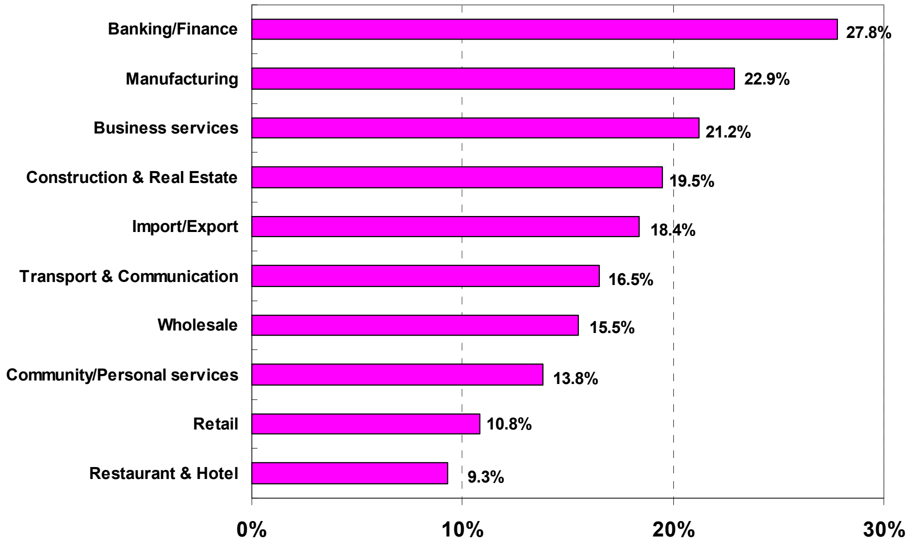
Although the overall security level has improved, the low security level witnessed in small companies signifies an area of concern. As many of these companies are less technology competent, they are more vulnerable to computer attacks and subsequent damages.

Table 3: Security level by staff size (2001-2002)

	1-19		*20-99*		*100 or above*	
	2001	**2002**	**2001**	**2002**	**2001**	**2002**
None	14.3%	11.6%	3.2%	4.2%	0%	5.9%
Basic	77.3%	64.9%	52.6%	31.7%	27.6%	11.8%
Firewall	8.0%	15.3%	20.7%	13.7%	13.8%	8.8%
Advanced	0.4%	8.2%	23.5%	50.5%	58.6%	73.5%
Total	100%	100%	100%	100%	100%	100%

In terms of industry sector, "Banking/Finance", "Manufacturing" and "Business services" sectors were better prepared for the attacks, with 27.8%, 22.9% and 21.2% adopting Advanced security technologies correspondingly (see Figure 6).

Figure 6: Advanced security level by industry sector



Source: HKCERT 2002

Computer attacks

The current study showed that around half of the interviewed companies (51.7%) had installed servers and/or web sites. Of these companies, 21% (326 out of 1,552 companies) experienced computer attacks within the last 12 months. Slightly over half of them (53.1%) reported 2-4 incidents and 30.7% mentioned once.

The total number of incidents recorded in the sample decreased from 1,387 incidents in 2001 to 1,095 incidents in 2002, down by 21.1%. In addition, the average number of attacks per victimized company dropped marginally from 3.5 times in 2001 to 3.4 times in 2002 (see Table 4).

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

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

Though the total number of incidents and average number of attacks per victimized company have decreased, the seriousness of computer attacks is on the rise (see Table 5).

In 2001, a total of 5,366 PCs were affected whereas the number increases to 5,460 in 2002, up by 1.8%. The average number of PCs affected per incident also rose from 3.9 to 5 over the past one year.

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

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

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 (2000-2002)

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

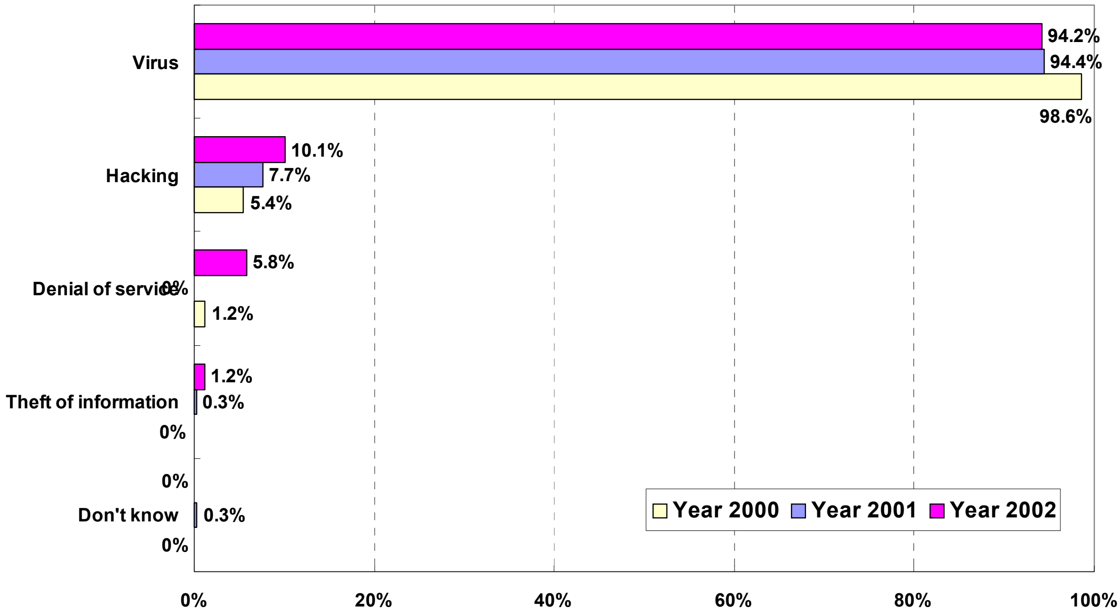
Table 6 shows that the average number of PCs affected per incident increases within all size groups in 2002. The increments are most evident among medium-sized and large companies.

However, in terms of the impact per computer attack, it is found that small companies suffered a much larger impact (0.46) than larger companies (0.31).

Tables 5 & 6 reinforce the statement that the extend and impact of computer attack has widen.

Computer virus (94.2%) is still the most prevailing type of computer attack. It is also worthy to note that the number of hacking has been rising continuously while denial of service has grown over the past one year.

Figure 7: Types of computer attack (2000-2002)



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

Source: HKCERT 2002

Magnitude of financial loss has enlarged in 2002. In the current study, a sum of HK$1.84 million was recorded among those companies that suffered from computer attacks, up by 20.5% from 2001 (see Table 7). This indicates that computer attacks are causing bigger losses and companies should pay more attention to protect their computer systems.

As virus remained the dominant type of attack, it explained 73.7% of the monetary loss, equivalent to a sum of HK$1.35 million. However, the damages caused by the more serious cyber crimes such as hacking, denial of service and theft of information should not be ignored as the financial loss from these attacks is increasing exponentially.

In this survey, 54% of the respondents reported financial loss resulted from the incidents. This figure is much higher when compared with that in 2001 (37.4%) and 2000 (13.3%) (see Table 8).

On top of the seriousness of the computer attacks, the increase of financial loss can be explained by the better alertness on hidden costs such as labor and time costs. In fact, failure to quantifying the financial impact will make companies underestimate the damages resulted from computer attacks and hence overlook the importance of information security.

Table 7: Financial losses by type of computer attack within the last 12 months (2000-2002)

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

Table 8: No. of incidents by type of computer attack within the last 12 months (2000-2002)

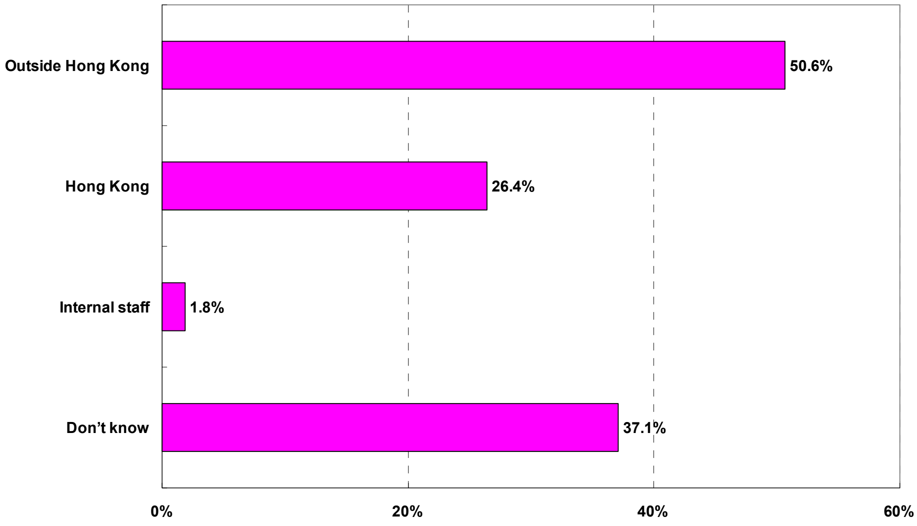
Type of computer attack	***No. of incidents***		
	Year 2000	*Year 2001*	*Year 2002*
Hacking	30	30	33
Denial of service	7	0	19
Virus	551	370	307
Theft of information	0	1	4
TOTAL	***588***	***401***	***363***
% of incidents reported financial loss	**13.3%**	**37.4%**	**54%**

Sources of attack

This report identified three main sources of attack, namely outside Hong Kong, Hong Kong and internal staff. The survey results show that around half of the attacks were from overseas while 26.4% were from Hong Kong. Only 1.8% of the attacks came from internal staff.

Quite many respondents (37.1%) 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. Knowing the source of attack can help formulate the suitable protection strategy.

Figure 8: Sources of attack



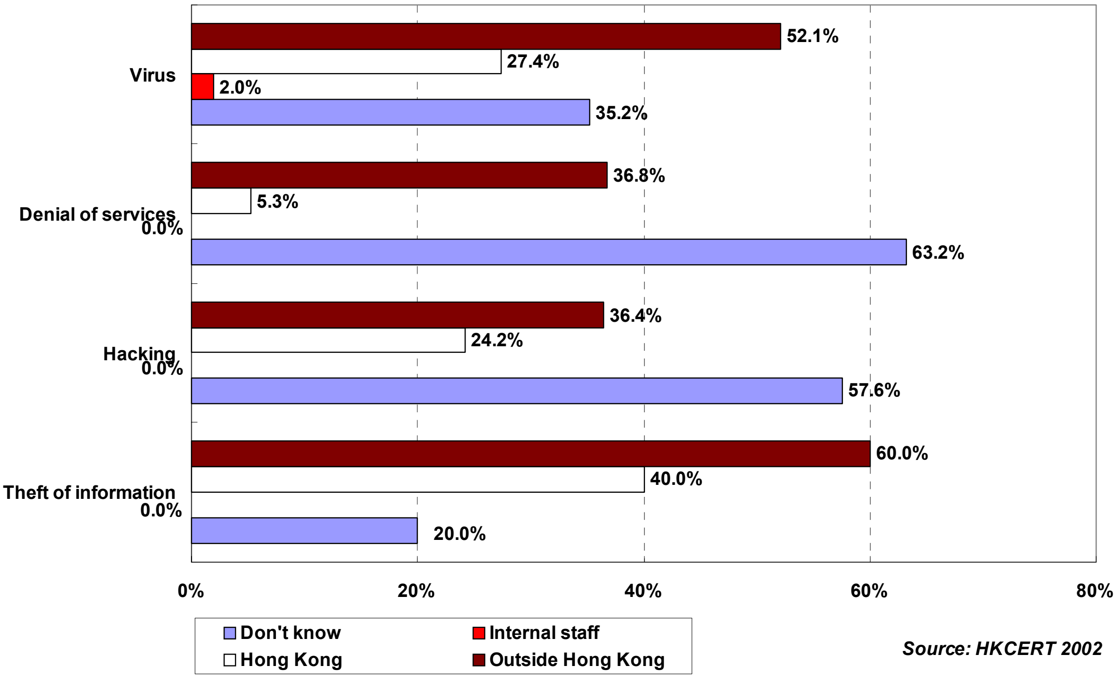
n = 326 companies suffered from computer attacks in the last 12 months

Source: HKCERT 2002

When we look into the sources of attack by type, we can find that only 5.3% of denial of services and 24.2% of hacking were from Hong Kong (see Figure 9). Both figures were lower than the percentage of attacks from Hong Kong shown in Figure 8.

Although the findings indicate that the risk of serious attacks by local competitors and hackers is not high, local companies should continuous to pay attention and be proactive to prevent any kinds of attacks.

Figure 9: Sources of attack by type



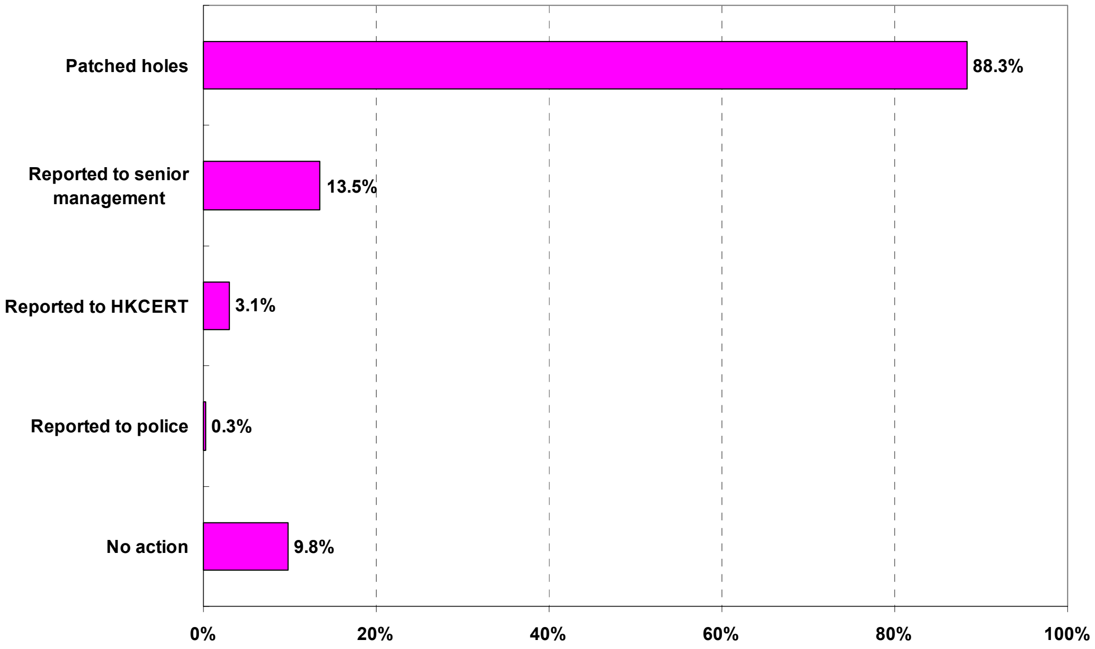
Source: HKCERT 2002

Actions against computer attacks

When asking how to deal with the attacks, most of the respondents (88.3%) replied that they would patch the security holes.

Only a few chose to report to HKCERT (3.1%) or the police (0.3%). Even worse, 9.8% had taken no actions at all against computer attacks.

Figure 10: Actions against computer attacks

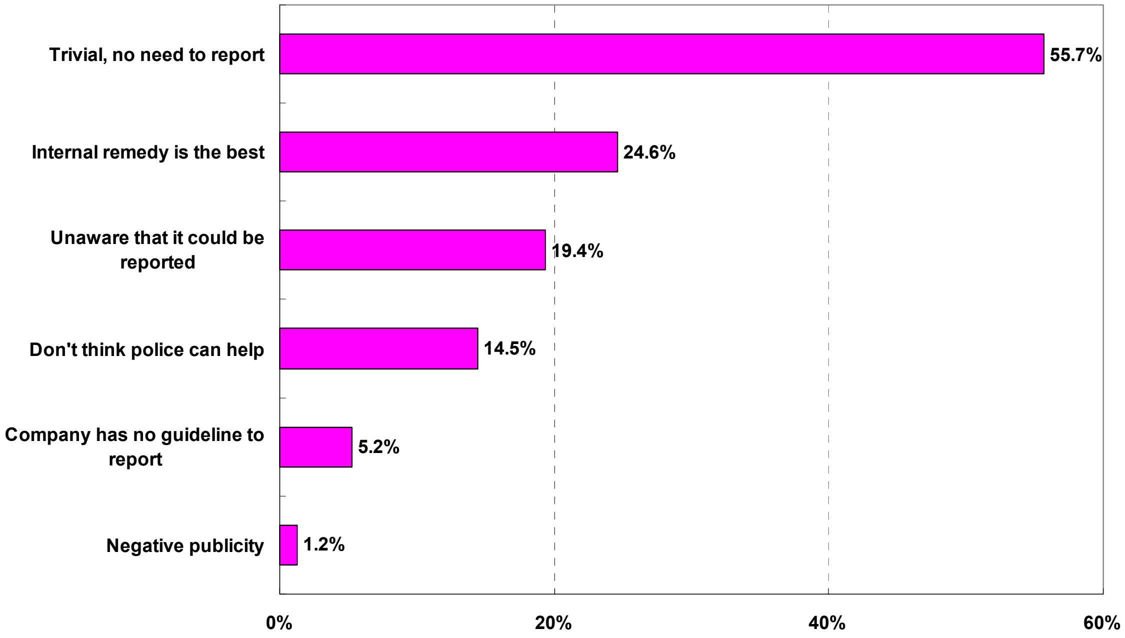


n = 326 companies suffered from computer attacks in the last 12 months

Source: HKCERT 2002

The key reason for not reporting to the police was found to be "Trivial, no need to report" (55.7%). "Internal remedy is the best" (24.6%) and "Unaware that it could be reported" (19.4%) were two other more frequently mentioned answers.

Figure 11: Reasons of not reporting to police

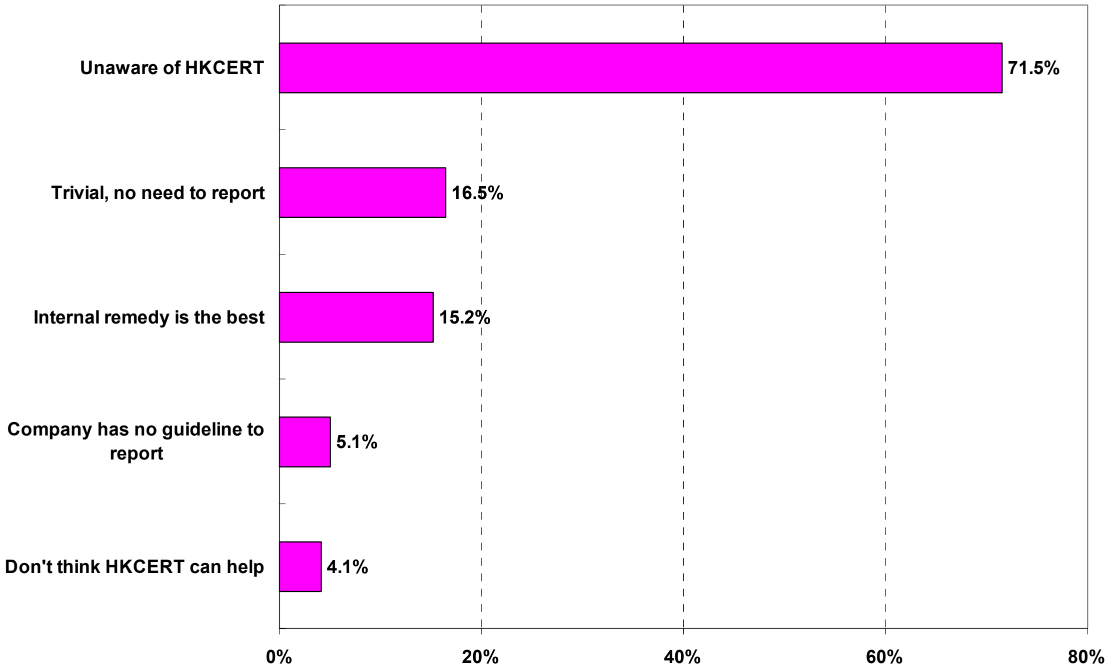


n = 325 respondents who had not reported to police after computer attacks *Source: HKCERT 2002*

Respondents did not report to HKCERT mainly because they were not aware of HKCERT (71.5%). Some considered that the attacks were trivial and did not need to be reported to HKCERT (16.5%) and some believed that internal remedy was the best (15.2%) (see Figure 12).

Many people, nowadays, are still unaware of the seriousness of computer attack and overlook its damages. Raising public awareness is crucial to prevent security breaches.

Figure 12: Reasons for not reporting to HKCERT



n = 316 respondents who had not reported to HKCERT after computer attacks *Source: HKCERT 2002*

Information security policy

Fourteen per cent of the interviewed companies have an information security policy in place, providing guidelines for their staff to follow in case of computer attacks.

Relatively speaking, large companies are more proactive in tackling computer attacks. Table 9 demonstrates that there is a positive relationship between the implementation of information security policy and the company size.

Table 9: Implementation of information security policy by staff size

Staff size	*Information security policy*
1-19	9.5%
20-99	30.8%
100 or above	58.8%
All companies	**14.2%**

In terms of industry sector, more companies in "Banking/Finance" (30.4%), "Restaurant & Hotel" (20.6%) and "Manufacturing" (18.2%) sectors had implemented information security policy (see Table 10).

Table 10: Implementation of information security policy by industry sector

Industry sector	*Information security policy*
Banking/Finance	30.4%
Restaurant & Hotel	20.6%
Manufacturing	18.2%
Business services	16.3%
Community/Personal services	14.2%
Import/Export	13.4%
Transport & Communication	11.9%
Retail	10.6%
Construction & Real Estate	9.7%
Wholesale	7.7%
All sectors	**14.2%**

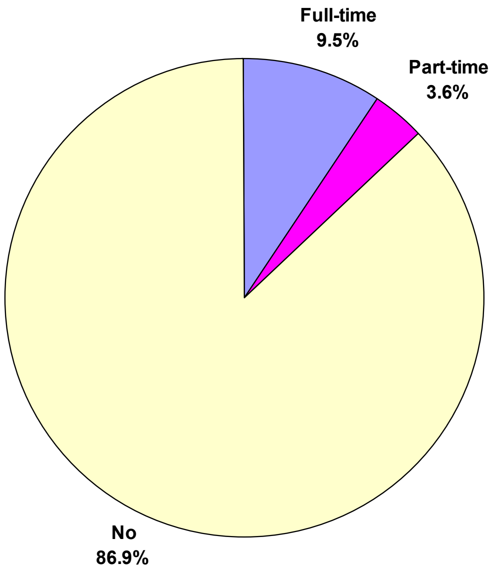
Information security staff

Nearly 10% of the surveyed companies employed full-time staff to deal with the information security issues while 3.6% hired part-time staff (see Figure 13). The majority (86.9%), however, did not have any people to handle the information security issues.

Large companies are more inclined to employ full-time or part-time staff to look after their company systems to prevent computer attacks. Figure 14 shows that 64.7% of the large companies had full-time or part-time staff responsible for information security whereas only 8% of small enterprises hired full-time or part-time information security staff.

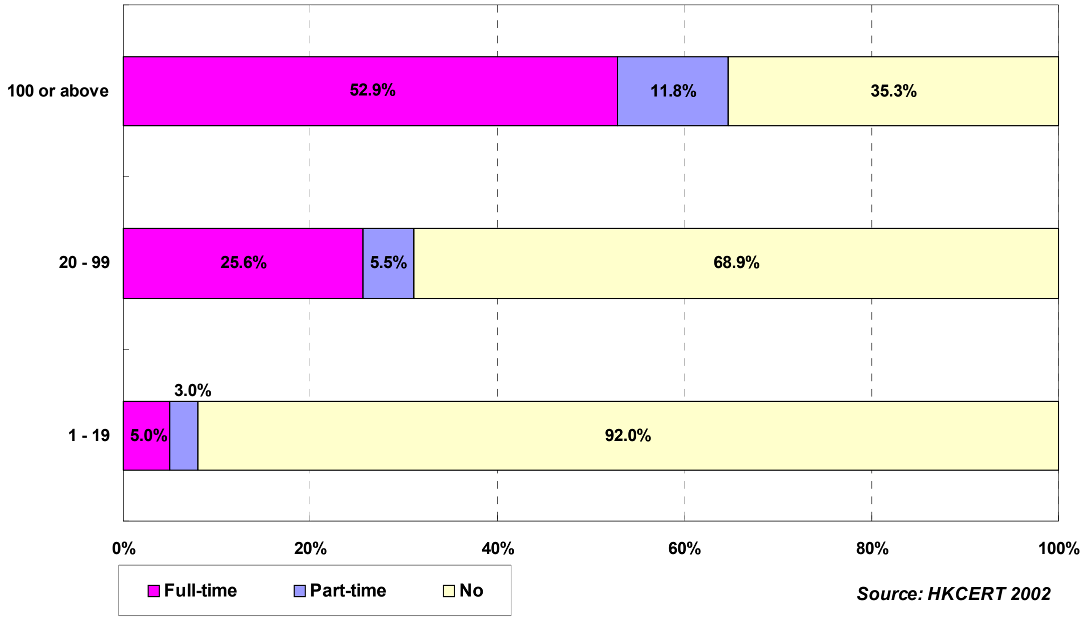
As illustrated in Figure 15, a noticeably high percentage of enterprises in "Manufacturing" (25%) and "Banking/Finance" (24.1%) sectors employed full-time or part-time staff to handle the information security issues.

Figure 13: In-house information security staff



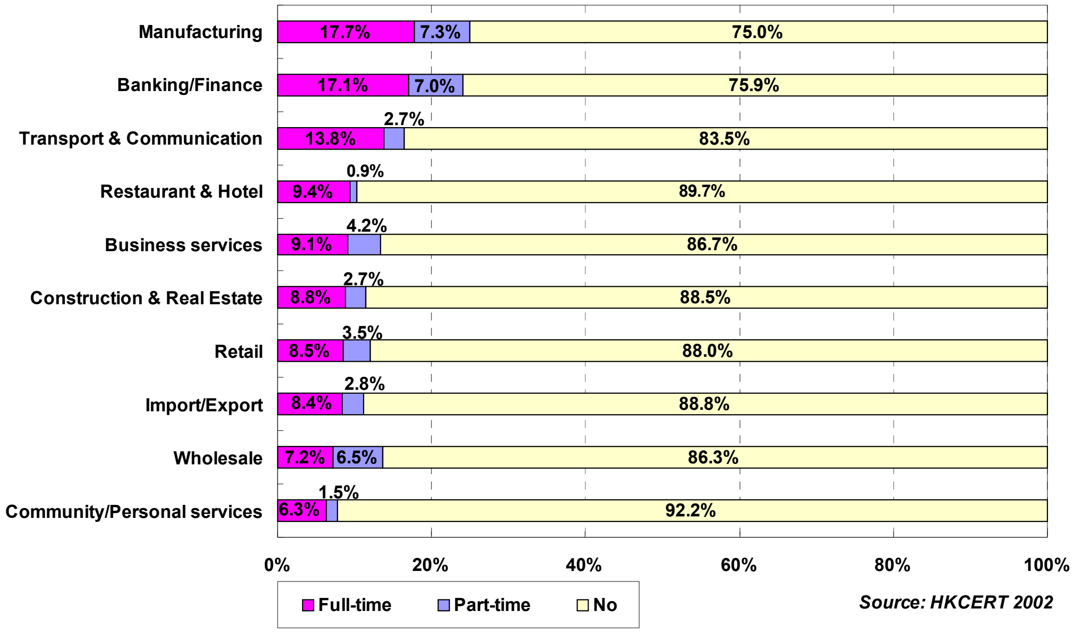
Source: HKCERT 2002

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



Source: HKCERT 2002

Figure 15: In-house information security staff by industry sector



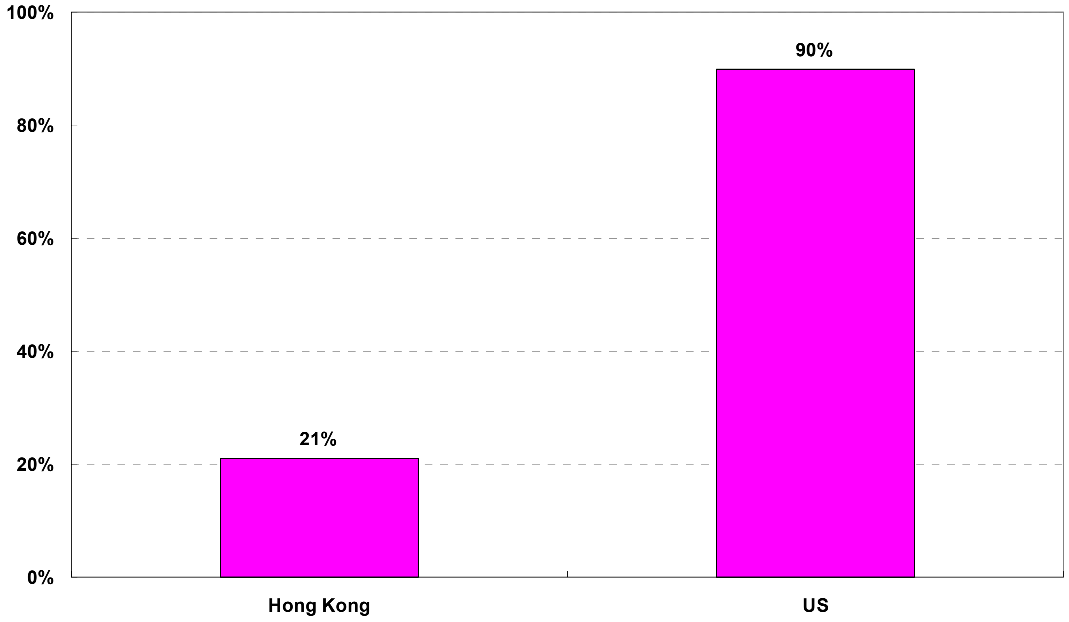
Source: HKCERT 2002

Comparison with United States

A similar survey conduced by Computer Security Institute (CSI) this year discovered that 90% of 503 companies surveyed in the United States (US) reported computer attacks in the past 12 months. Figure 16 illustrates that the percentage is much higher than that of Hong Kong (21%).

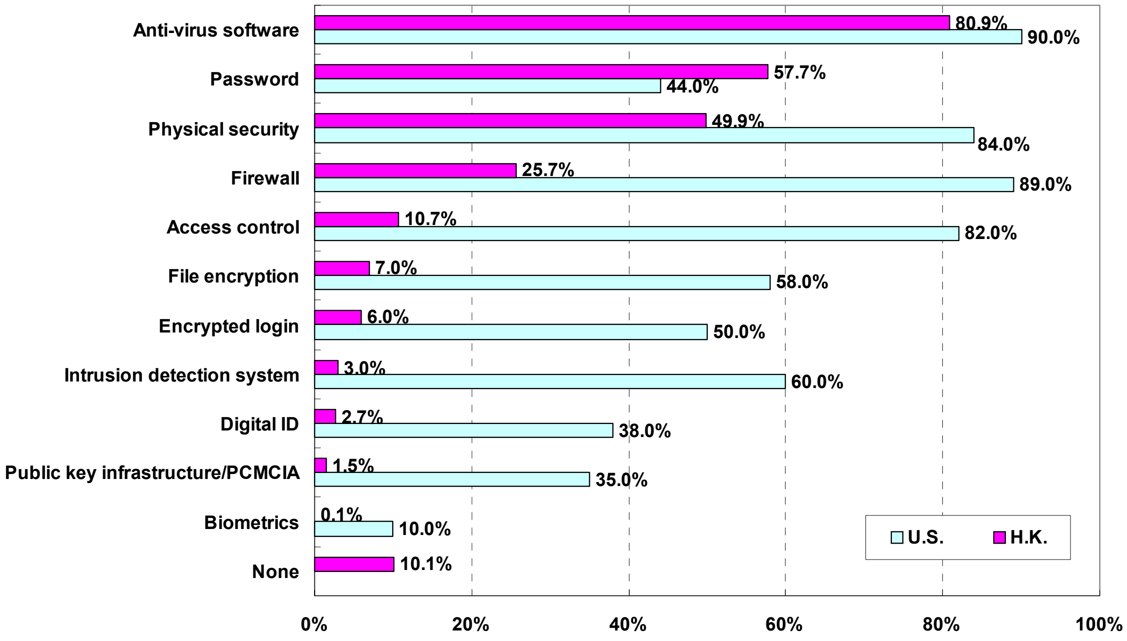
Overall speaking, given the higher computerization level and security concern in US, along with more cyber crimes and the possibility of higher financial losses, US companies adopted more sophisticated security technologies than those in Hong Kong (see Figure 17).

Figure 16: Computer attacks in Hong Kong and US



Source: HKCERT & CSI 2002

Figure 17: Security technologies adopted in Hong Kong and US



Source: HKCERT & CSI 2002

Summary Findings

Security technology

- Ninety per cent of the surveyed companies had adopted security technologies.
- The three most common measures were "Anti-virus software" (80.9%), "Password" (57.7%) and "Physical security" (49.9%).
- The overall security level had improved over the past two years. However, the security level in small companies was still low with 11.6% having no security technology in place and 64.9% belonged to the Basic level.
- More companies in "Banking/Finance" (27.8%), "Manufacturing" (22.9%) and "Business services" (21.2%) sectors adopted Advanced security technologies.

Computer attacks

- Around half of the respondents (51.7%) expressed that their companies had servers and/or web sites.
- Of these companies, 21% experienced computer attacks within the last 12 months.
- The total number of incidents recorded in the sample was 1,095 and the average number of attacks per victimized company was 3.4 times.
- A total of 5,460 PCs were affected and the average number of PCs affected per incident was 5.
- Small companies suffered a larger impact of computer attack, with a higher percentage of PCs being affected.
- "Virus" (94.2%) was the dominant form of computer attack.
- The financial loss resulted from computer attacks increased from HK$1.52 million in 2001 to HK$1.84 million in 2002, up by 20.5%.
- Damages caused by hacking, denial of service and theft of information increased remarkably.
- More than half of the attacks were from overseas (50.6%).

Actions against computer attacks

- Most of the companies suffered from computer attacks in the last 12 months had patched the security holes (88.3%) after the attacks. Only 3.1% and 0.3% had reported to HKCERT and the police respectively.
- "Trivial, no need to report" (55.7%), "Internal remedy is the best" (24.6%) and "Unaware that it could be reported" (19.4%) were the three major reasons for not reporting to the police.

- The reasons for not reporting to HKCERT were “Unaware of HKCERT” (71.5%), “Trivial, no need to report” (16.5%) and “Internal remedy is the best” (15.2%).

Information security policy

- Fourteen per cent of the surveyed companies had information security policy in place.
- Nearly 10% of the surveyed companies employed full-time staff to handle the information security issues while 3.6% hired part-time staff.

Figures at a glance – 2000 to 2002

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