

Information Security Survey 2001

October, 2001

Published by:



© 2001. 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. HKPC 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 and level of security awareness in Hong Kong, Hong Kong Productivity Council (HKPC) has planned to carry out a series of studies on information security since 2000.

This is the second time HKPC conducted such kind of study. This report not only presents detailed findings from the current study but also compares the results in 2000.

Objectives

This study explores the information security status in Hong Kong in 2001. Specifically, this study aims to:

- Serve as an update of the previous survey conducted in October 2000;
- Investigate the types of computer attacks and their impacts;
- Understand the actions that companies have taken to deal with the attacks;
- Examine the latest security technologies adopted by companies in Hong Kong.

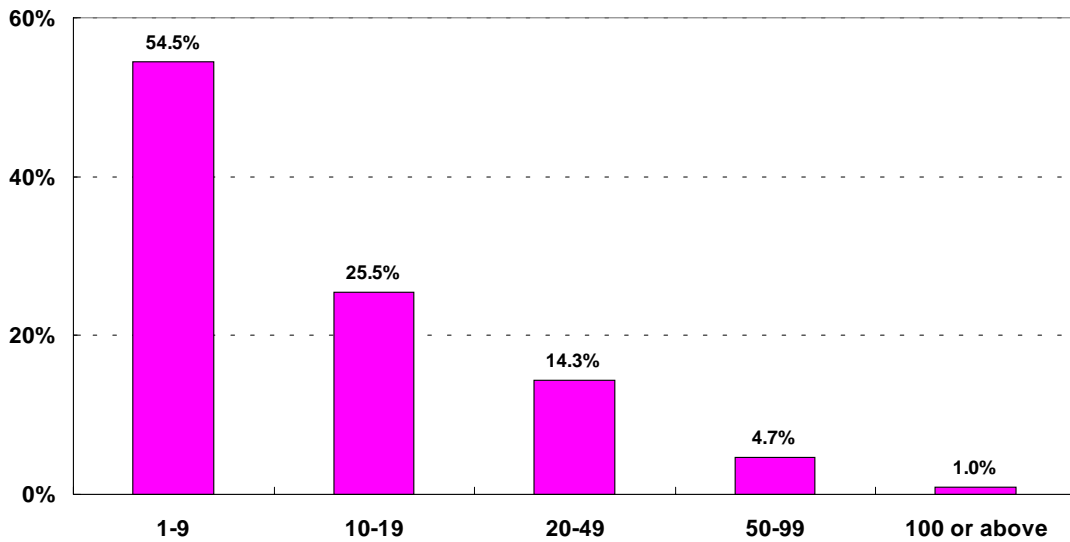
Methodology

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. Altogether 3,000 companies were successfully interviewed by telephone from July to August 2001.

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.

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

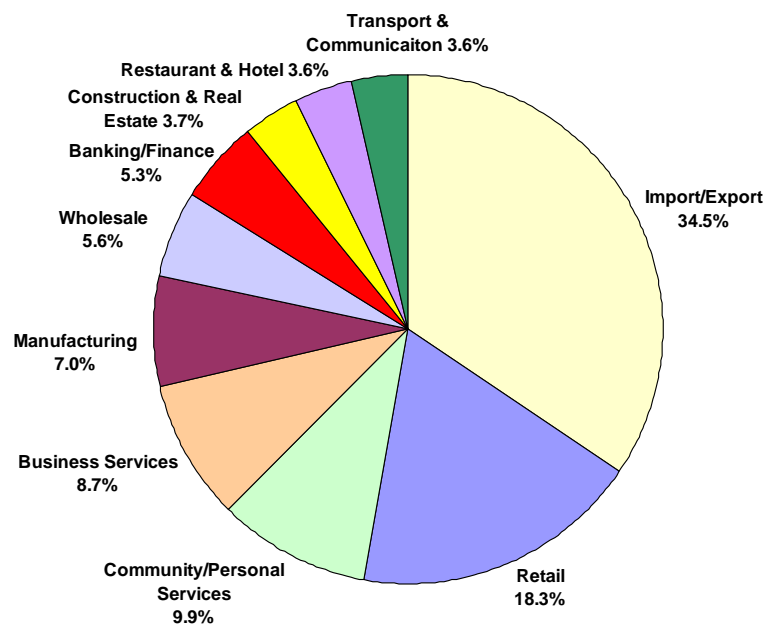
Figure 1: Sample distribution by staff size



Source: HKPC 2001

Slightly more than one-third of the sample units came from the Import/Export sector, followed by the Retail sector (18.3%). The distribution of the sample reflects the pattern seen in the community as a whole.

Figure 2: Sample distribution by industry sector



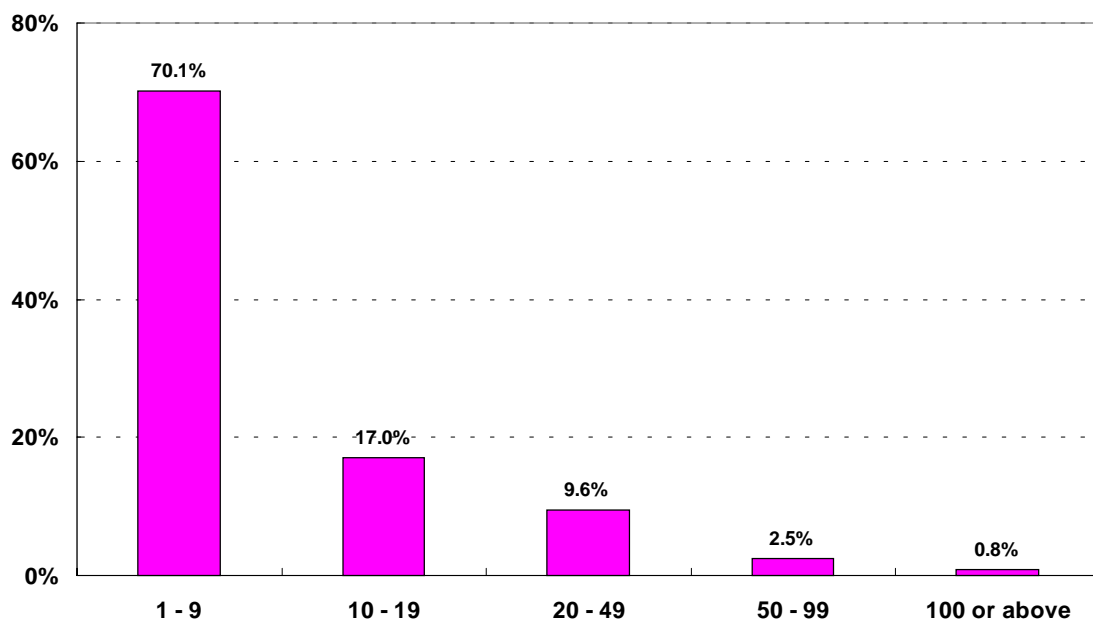
Source: HKPC 2001

Major Findings

Number of PCs installed

The number of personal computers (PCs) installed tends to be small in general, mainly due to the significant presence of small to medium-sized enterprises (SMEs). As illustrated in Figure 3, most interviewed companies (70.1%) had an installation base of 1-9 units. Only 0.8% had more than 100 PCs.

Figure 3: Number of PCs installed



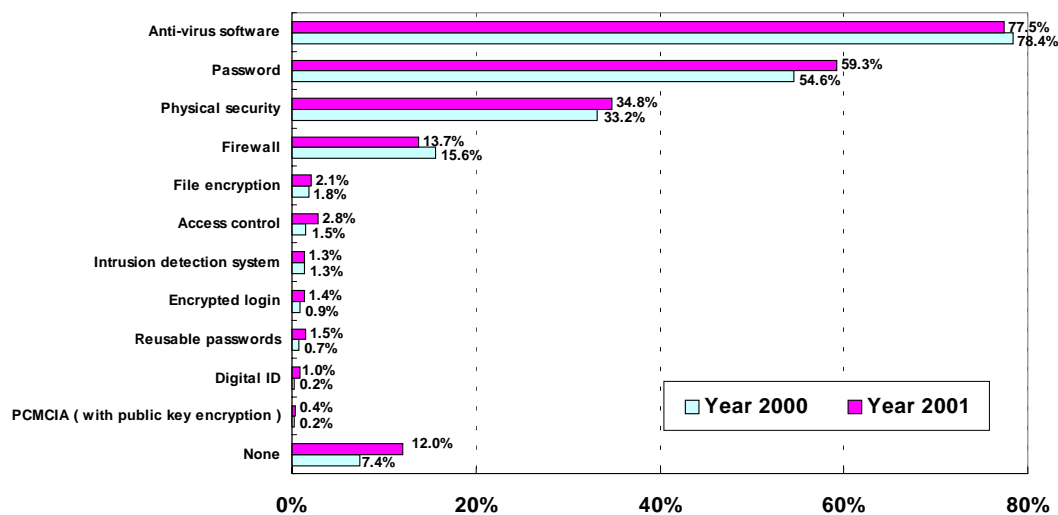
Source: HKPC 2001

Security technology

Nearly 90% of the interviewed companies had adopted security technologies for safeguarding their company information. The three most popular measures were “Anti-virus software” (77.5%), “Password” (59.3%), and “Physical security” (34.8%). However, 12% of the interviewed companies did not use any security technologies. The distribution pattern is similar to that in 2000 (see Figure 4).

For the security technology adopted by staff size, please refer to Table 1.

Figure 4: Security technology adopted (2000-2001)



Source: HKPC 2001

Table 1: Security technology adopted by staff size (2000-2001)

	1-19		20-99		100 or above	
	2000	2001	2000	2001	2000	2001
Anti-virus software	75.9%	73.9%	85.6%	91.6%	100%	93.1%
Password	50.4%	53.4%	66.6%	82.3%	95.7%	93.1%
Physical security	31.2%	29.2%	39.6%	56.2%	39.1%	79.3%
Firewall	11.7%	8.1%	26.7%	35.2%	56.5%	55.2%
File encryption	0.7%	0.1%	3.8%	8.9%	47.8%	37.9%
Access control	0.8%	0.2%	2.4%	11.4%	43.5%	44.8%
Intrusion detection system	0.4%	0.0%	3.7%	6.1%	17.4%	13.8%
Encrypted login	0.4%	0.0%	2.1%	6.5%	8.7%	13.8%
Reusable passwords	0.3%	0.0%	1.4%	6.5%	21.7%	24.1%
Digital ID	0.2%	0.1%	0.1%	3.7%	8.7%	10.3%
PCMCIA	0.0%	0.0%	0.6%	1.8%	4.3%	3.4%
None	8.9%	14.3%	2.8%	3.2%	0.0%	0.0%
Total	180.9%	179.3%	235.4%	313.4%	443.4%	468.8%

Security level

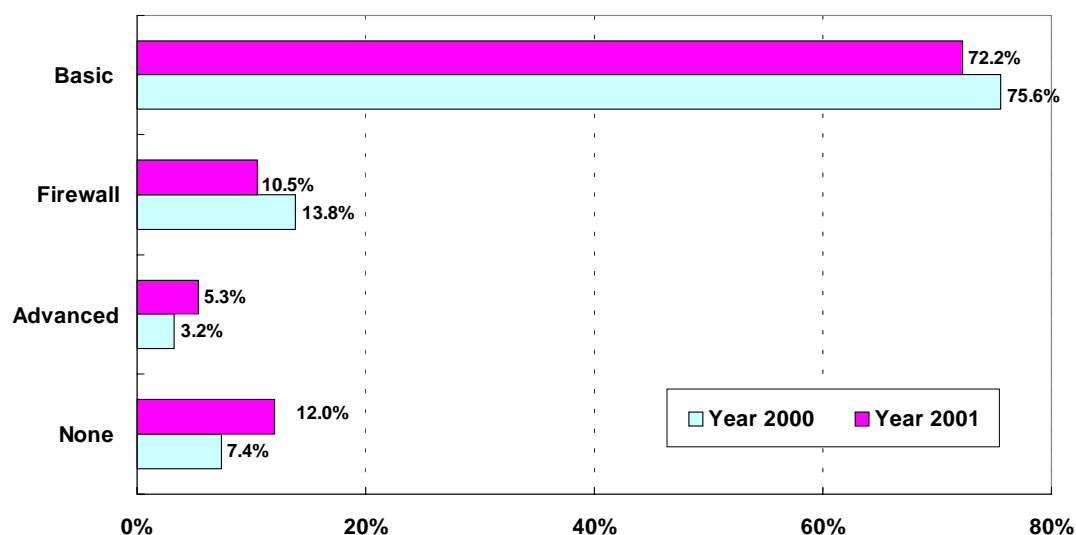
For further analysis purpose, all security technologies listed in this survey were classified into four levels, namely None, Basic, Firewall and Advanced. Detailed explanations are listed in Table 2.

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 <i>with/without</i> Basic level of security technology
Advanced	File encryption/Access control/Intrusion detection system/ Encrypted login/Reusable passwords/Digital ID/PCMCIA <i>with/without</i> lower levels of security technology

As shown in Figure 5, 72.2% of the surveyed companies deployed Basic security measures and only 5.3% employed Advanced security technologies in 2001.

Figure 5: Security level (2000-2001)



Source: HKPC 2001

The security level correlates with the staff size. Among the small companies surveyed, the use of Basic security measures was dominant (77.3%) whereas nearly three-fifths of the large enterprises utilized Advanced security technologies to prevent security breaches in 2001 (see Table 3).

Compared with the previous findings, security level is improving among medium-sized and large companies, with more companies having adopted higher level of security technologies in 2001. However, small companies still lack the initiative to protect their computer systems from attacks. The percentage of not having any security technologies in place among small companies increased slightly from 8.9% in 2000 to 14.3% in 2001.

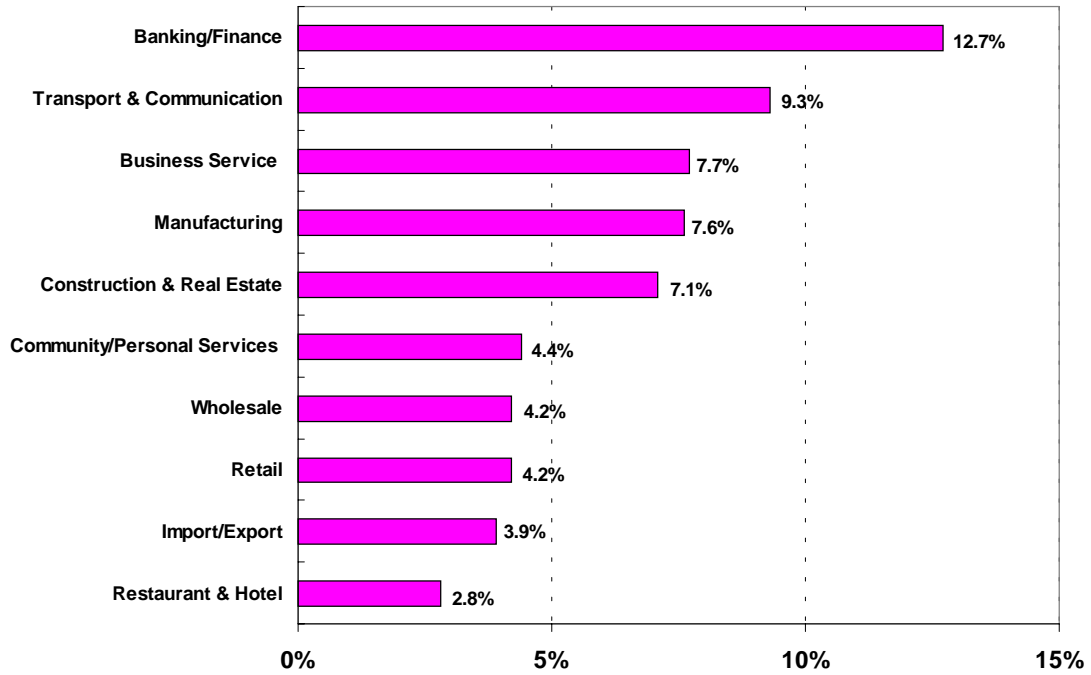
The low security level witnessed in small companies signifies an area of concern. As many of these companies do not have an IT department nor even a full-time IT staff, they are less technically competent and thus more vulnerable to computer attacks and subsequent damages.

Table 3: Security level by staff size (2000-2001)

	1-19		20-99		100 or above	
	2000	2001	2000	2001	2000	2001
None	8.9%	14.3%	2.8%	3.2%	0%	0%
Basic	78.6%	77.3%	67.3%	52.6%	34.8%	27.6%
Firewall	11.0%	8.0%	22.8%	20.7%	8.7%	13.8%
Advanced	1.5%	0.4%	7.1%	23.5%	56.5%	58.6%
Total	100%	100%	100%	100%	100%	100%

In terms of industry sector, “Banking/Finance” sector were more proactive in protecting itself from being attacked, with 12.7% adopting Advanced security technologies (see Figure 6).

Figure 6: Advanced security level by industry sector



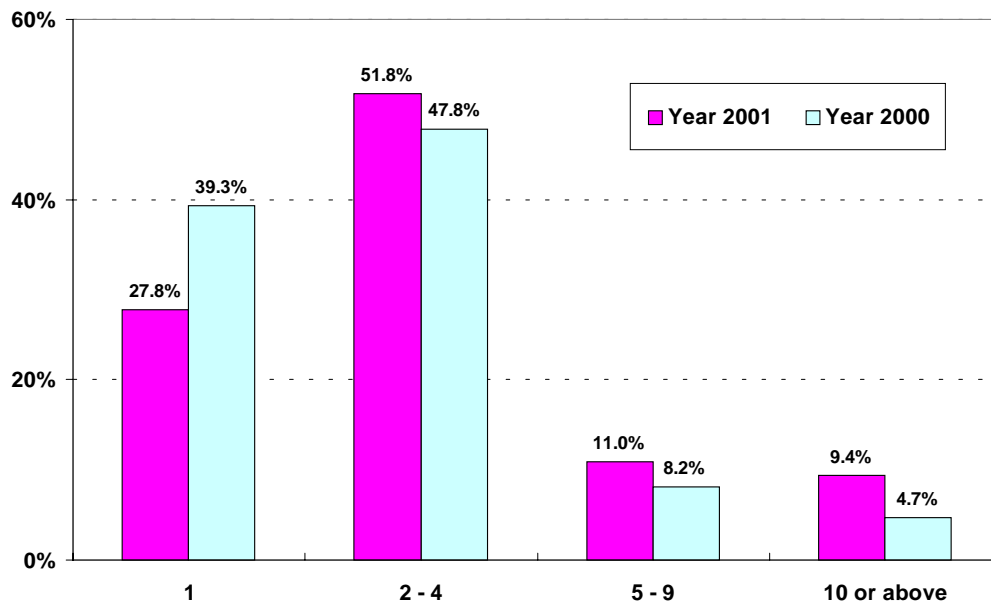
Source: HKPC 2001

Computer attacks

Around half of the respondents (1,517 respondents) indicated that their companies had installed servers and/or web sites. Of these companies, 25.8% (392 respondents) experienced computer attacks within the last 12 months. Slightly over half of the respondents reported 2-4 incidents (51.8%) and 27.8% cited once (see Figure 7).

The total number of incidents recorded in the sample decreased from 1,510 incidents in 2000 to 1,387 incidents in 2001, down by 8.1%. However, the average number of attacks per victimized company rises from 2.6 times in 2000 to 3.5 times in 2001, signifying an upward shift that calls for attention.

Figure 7: Number of computer attacks (2000-2001)



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

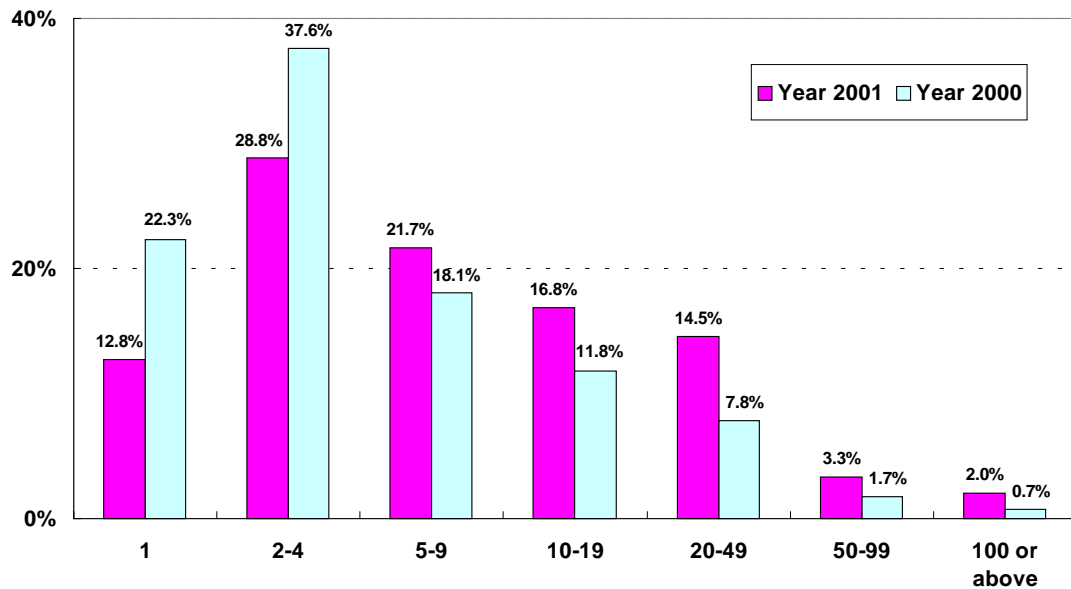
Source: HKPC 2001

Figure 8 compares the number of PCs affected by computer attacks in 2000 and 2001. Three-fifths of the victimized companies stated that more than 4 PCs were affected in the past 12 months in 2001.

In the past study, a total of 4,733 PCs were affected whereas the number increases to 5,366 in 2001, up by 13.4%. The average number of PC affected per incident also rose from 3.1 to 3.9 over the past one year.

Companies should not ignore the consequences caused by computer attacks.

Figure 8: Number of PCs affected by computer attack (2000-2001)



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

Source: HKPC 2001

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 4: Extent and impact of computer attack (2000-2001)

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

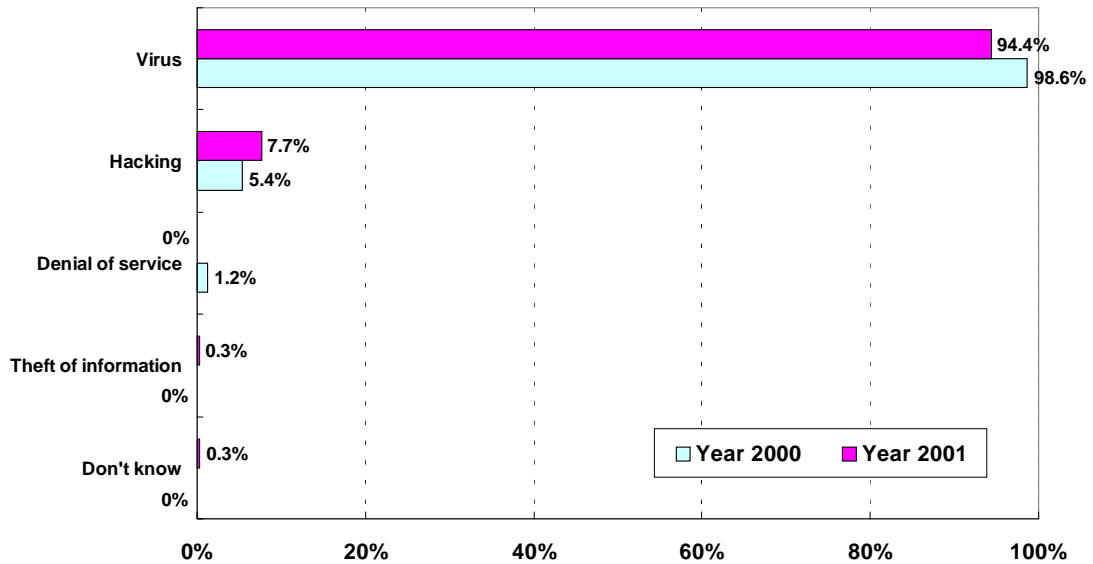
Table 4 shows that the average number of PCs affected per incident increases within all size groups in 2001. The increments are most evident among medium-sized and large companies.

In terms of the impact per computer attack, it is found that SMEs suffered a much larger impact than large companies. In particular, the percentage of PCs suffered per attack in small entities was nearly three to four times that of large organizations. Compared with the figures in 2000, the impact per computer attack increases marginally in every size group in 2001.

This reinforces the statement that the extend and impact of computer attack has widen.

Survey data revealed that computer virus (94.4%) continues to be the most prevailing type of computer attack in 2001. It is also worthy to note that hacking has increased from 5.4% to 7.7% over the past one year.

Figure 9: Types of computer attack (2000-2001)



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

Source: HKPC 2001

Regarding the financial loss, a sum of HK\$1.52 million was recorded among those companies that suffered from computer attacks in 2001. The amount is 10.8% higher than that in 2000 (see Table 5). This indicates that computer attacks are causing bigger losses and companies should pay more attention to the protection of their IT systems.

As virus remained the dominant type of attack, it explained 94.9% of the monetary loss, equivalent to a sum of HK\$1.45 million.

In this survey, 37.4% of the respondents reported financial loss resulted from the incidents. This figure is much higher when compared with that in 2000 (13.3%) (see Table 6).

However, many respondents still do not take into account of the labor and time costs incurred in system recovery. 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 5: Financial losses by type of computer attack within the last 12 months (2000-2001)

Type of computer attack	Total financial loss (HK\$)	
	Year 2000	Year 2001
Hacking	116,000	77,500
Denial of service	0	0
Virus	1,259,650	1,446,500
Theft of information	0	0
TOTAL	1,375,650	1,524,000
Average Financial Loss per Victimized Company	2,461	3,888

Table 6: No. of incidents by type of computer attack within the last 12 months (2000-2001)

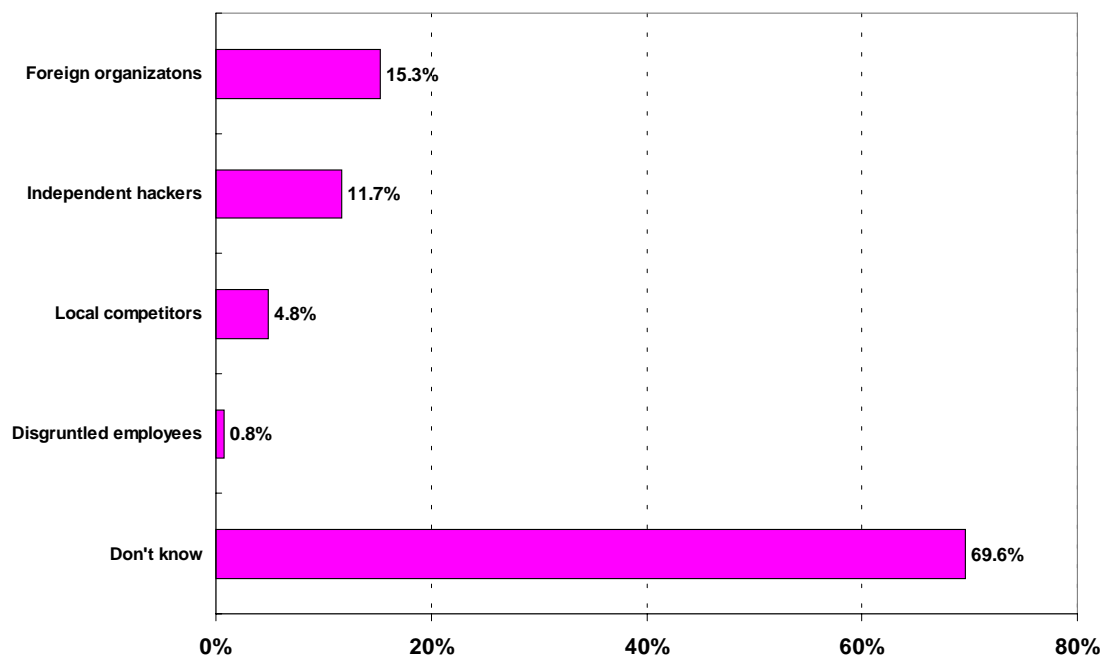
Type of computer attack	No. of incidents	
	Year 2000	Year 2001
Hacking	30	30
Denial of service	7	0
Virus	551	370
Theft of information	0	1
TOTAL	588	401
% of incidents reported financial loss	13.3%	37.4%

Sources of attack

This report identifies four main sources of attack, namely Foreign Organization, Independent Hackers, Local Competitors and Disgruntled Employees. Foreign Organizations (15.3%) and Independent Hackers (11.7%) appeared to be the more common sources. Only 0.8% of the attacks came from disgruntled employees (see Figure 10).

However, many of the respondents (69.6%) did not know the origin of the attacks. As the attacks can strike at any time, from anywhere, by anyone, proactive measures that protect the company's information or actions to investigate the source of attacks should be taken properly.

Figure 10: Sources of attack



n = 392 companies suffered from computer attacks in the last 12 months

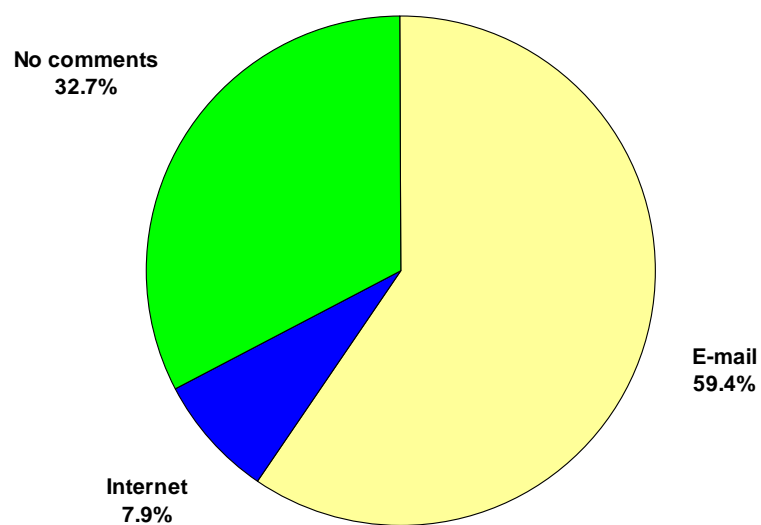
Source: HKPC 2001

Means of attack

About three-fifths of the interviewed companies had been attacked via e-mails.

In a connected economy, e-mails are widely used for communication in both business and social sectors. On the other hand, it can be a convenient and efficient means of attack. Therefore, companies should develop a security policy and measures regarding the use of e-mail to protect themselves.

Figure 11: Means of attack



n = 392 companies suffered from computer attacks in the last 12 months

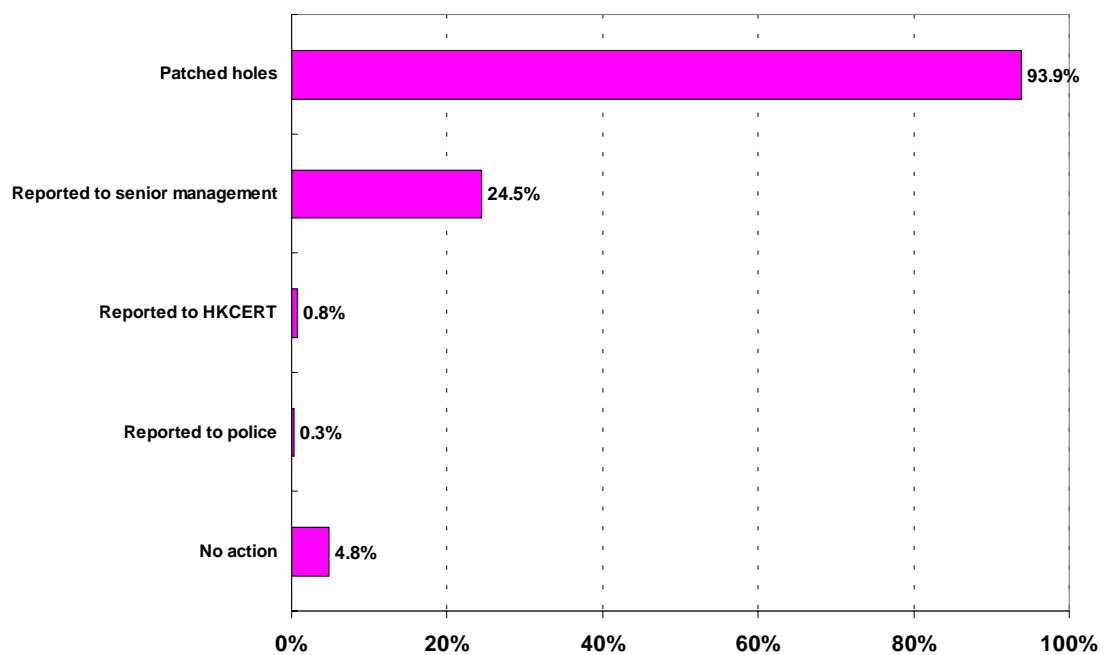
Source: HKPC 2001

Actions against computer attacks

When asking how to deal with computer attacks, most of the respondents (93.9%) said that they would patch the security holes. The figure is much higher than that in 2000 (78.3%).

Only a few chose to report to Hong Kong Computer Emergency Response Team (HKCERT) (0.8%) or the police (0.3%). Even worse, 4.8% had taken no actions at all against computer attacks.

Figure 12: Actions against computer attacks



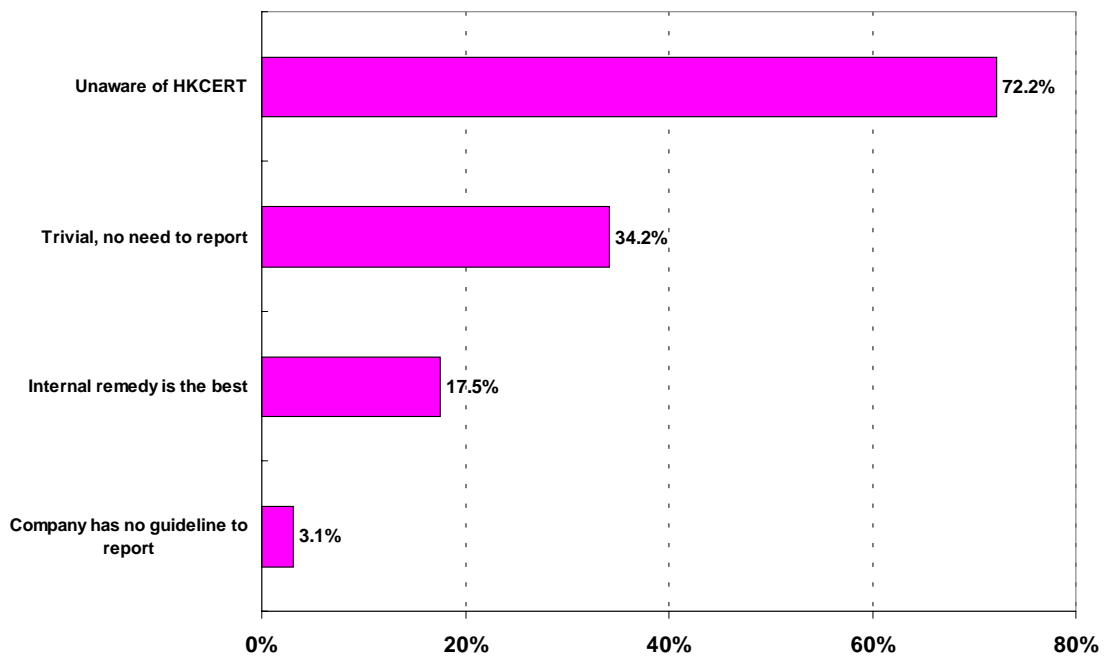
n = 392 companies suffered from computer attacks in the last 12 months

Source: HKPC 2001

The key reason for not reporting to HKCERT was found to be “Unaware of HKCERT” (72.2%). Thirty four per cent considered the attacks were trivial matters and so there was no need to report to HKCERT (see Figure 13).

Many people, nowadays, are still unaware of the seriousness of computer attack and overlook its damages. Importance of information security and user education has to be promoted.

Figure 13: Reasons for not reporting to HKCERT



n = 389 respondents who had not reported to HKCERT after computer attacks

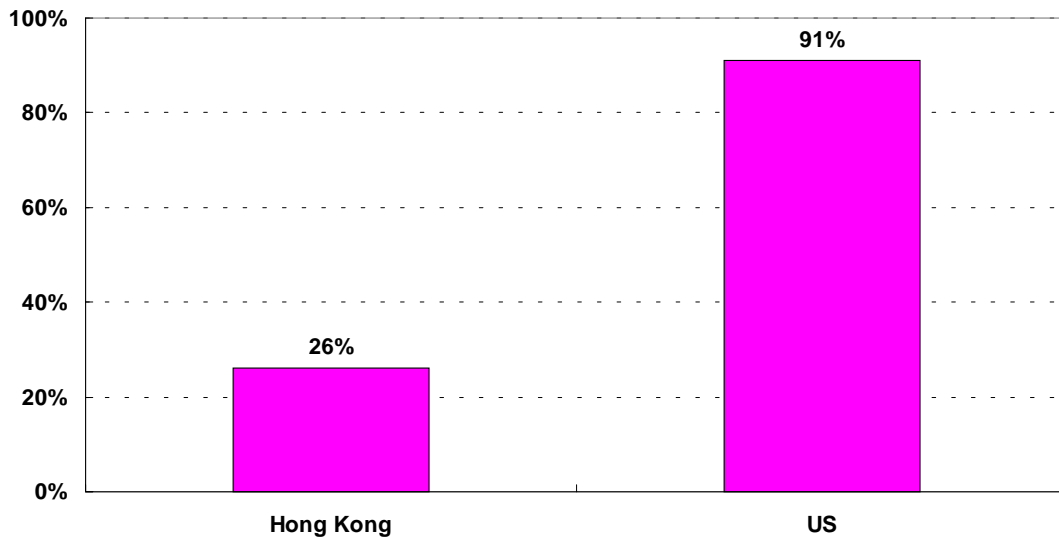
Source: HKPC 2001

Comparison with United States

A similar survey conducted by Computer Security Institute (CSI) this year discovered that 91% of 538 companies surveyed in the United States (US) reported that their computers had been attacked in the past 12 months. Figure 14 illustrates that the percentage is much higher than that of Hong Kong (26%).

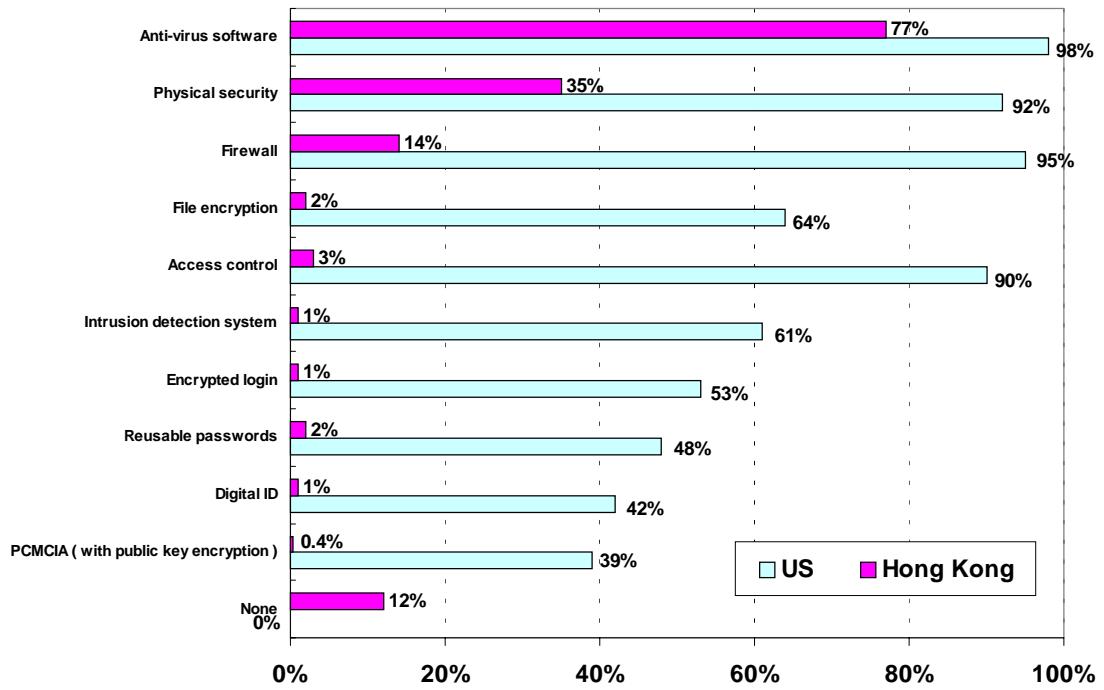
Overall speaking, given the higher computerization level and security concern in US, US respondents adopted more sophisticated security technologies than those in Hong Kong (see Figure 15).

Figure 14: Computer attacks in Hong Kong and US



Source: HKPC & CSI 2001

Figure 15: Security technologies adopted in Hong Kong and US



Source: HKPC & CSI 2001

Summary Findings

Security technology

- The majority of respondents (88%) had deployed security technologies in their organizations. The most common measures were “Anti-virus software” (77.5%), “Password” (59.3%) and “Physical security” (34.8%).
- Most of the surveyed companies (72.2%) adopted Basic security measures. Only 5.3% used Advanced security technologies.
- Overall speaking, the security level is higher amongst large companies. In terms of industry sector, “Banking/Finance” sector shows the highest percentage in adopting Advanced security technologies.
- 12% no technology at all.

Computer attacks

- Around half of the respondents expressed that their companies had servers and/or web sites.
- Of these companies, 25.8% had suffered from computer attacks in the past 12 months. On average, each victimized company recorded 3.5 incidents.
- SMEs suffered a larger impact of computer attack than large organizations, with a higher percentage of PCs being affected.
- “Virus” (94.4%) was the dominant form of computer attack.
- A total of 5,366 PCs was affected in the victimized companies in the past 12 months and the financial loss resulted from computer attacks amounted to HK\$1.52 million.
- The most likely sources of attack were “Foreign Organization” (15.3%) and “Independent Hackers” (11.7%). However, 69.6% of respondents did not know where the attacks came from.
- E-mail (59.4%) was the most common medium of attack.

Actions against computer attacks

- Most of the companies suffered from computer attacks in the last 12 months had patched the security holes after the attacks (93.9%). Around a quarter had reported to senior management. Only 0.8% had reported to HKCERT.
- “Unaware of HKCERT” (72.2%) and “Trivial, no need to report” (34.2%) were the two major reasons for not reporting to HKCERT.

Conclusion

Computer attack cannot be ignored. In this survey, though the total number of incidents recorded in the sample decreases, the total financial loss and the impact per computer attack within all the size groups increase when compared with the figures in 2000.

However, many companies, especially SMEs, still ignore the importance of information security. Some of them even treat computer attack as a trivial matter and thus pay little attention to it.

Given the growing popularity of the Internet and electronic commerce, information security should not be overlooked. This is particularly essential for companies that are doing or plan to do electronic commerce which requires a high level of data privacy and security.

To raise the public awareness of information security, user education, promotion and training are needed. In addition, companies should be encouraged to develop an information security policy and implement measures, addressing both the human and technical issues, to prevent computer attacks or minimize the financial loss after the incidents.

At a glance – Figures in 2000 and 2001

	Year 2000	Year 2001	% change
Total no. of incidents	1,510	1,387	-8.1%
Average no. of attacks per victimized company	2.6	3.5	+34.6%
Total no. of PCs affected	4,733	5,366	+13.4%
Average no. of PCs affected per incident	3.1	3.9	+25.8%
Total financial loss	HK\$1.38M	HK\$1.52M	+10.8%
Average financial loss per victimized company	HK\$2,461	HK\$3,888	+58%