

The logo features a central blue circle with a yellow sunburst border. The year '2003' is written in large, bold, red letters with a white outline. Below it, the text 'BSI Computer Theft Survey Results' is written in a smaller, bold, red font with a white outline, arranged in two lines.

**2003**  
**BSI Computer Theft**  
**Survey Results**

**Brigadoon Software<sup>inc</sup>**

---

## Table of Contents

Executive Summary.....	iii
The Survey.....	1
The Respondents .....	1
Age and Gender .....	2
Respondent Geographic Distribution .....	3
Respondents' Job Titles.....	4
Response Percent.....	5
Respondents organization's primary business .....	6
Response Percent.....	6
Anatomy of Computer Theft.....	7
Stolen: How Many Incidents .....	7
How Many Stolen .....	7
What Was Stolen.....	8
Operating Systems of Stolen Computers.....	8
When It Was Stolen.....	9
Where It Was Stolen .....	9
Where It Was Stolen: Stationary Locations.....	10
Where It Was Stolen: Academic Sector .....	11
Why It Was Stolen.....	12
The Cost of Computer Theft .....	13
Cost of the Computer .....	13
Average Hardware Cost.....	14
Total Replacement Cost of the Computer Replacement.....	15
Total Replacement Cost: Averages.....	16
Cost of Computer Theft: Downtime .....	16
The "Real" Cost of Computer Theft: Loss of Proprietary Data.....	17
Average Value of Proprietary Data.....	17
What Proprietary Data- Stolen Computers.....	18
What Proprietary Data- All Respondents' Computers .....	19
What Else Was Stolen .....	20
Computer Theft: Countermeasures .....	21
Countermeasures Utilized After Theft: Increased Usage of Tracking/Location Software.....	22
Data Backup .....	23
Backup: How Often .....	23
Organizations: Security Guidelines .....	24
Conclusions and Recommendations .....	25
Conclusions .....	25
Recommendations .....	26
About BSI .....	27
Reprint Guidelines .....	27

---

## Executive Summary

Key findings of the 2003 BSI Computer Theft Survey:

- ▶ Almost half (44.5%) of the survey respondents have been the victim of computer theft in the last 12 months.
- ▶ 53% of computer theft occurred while respondent was mobile (moving about), rendering cables, locks and enclosures virtually useless.
- ▶ Nearly three quarters (72.5%) of respondent companies had between 1 and 9 computers stolen in the last 12 months; nearly 1 in 10 (9.7%) respondent companies had more than 25 computers stolen in the last 12 months.
- ▶ Laptops comprised nearly half (48%) of those devices reported stolen, followed by desktop computers (26.7%) and PDAs (13.3%).
- ▶ 99% of survey respondents that experienced computer theft report the thief was never caught.
- ▶ 67.7% of respondents report the estimated value of proprietary data on their stolen computing device at \$25,000 or less; 9.2% estimated the value at \$1,000,000 or more and 2.3% estimated the value at more than \$10,000,000.
- ▶ The value of proprietary data on respondents' stolen computers averaged an astounding \$690,759.61 per stolen computer.
- ▶ 45.6% of respondents report other items were stolen at the time of the computer theft, with removable media (including spare disks, stored files on CDs, removable media and spare hard drives) accounting for 21.8 % of the additional stolen items.
- ▶ 92.7% of respondents use only a log-on password to protect their computer; 70% recorded and stored the make, model and serial number of the computer in case of theft; and almost one quarter (23.3%) used no security precautions to safeguard their computing device from theft.
- ▶ 68% of all respondents report they only back-up data weekly, monthly, rarely or never - making the theft of a computing device a serious event that results in the permanent loss of data.
- ▶ 88% of respondents did not encrypt the proprietary data on their stolen computing device.
- ▶ 46.7% of respondents that experienced computer theft had multiple incidences of theft in the last 12 months.
- ▶ Nearly two-thirds (63.5%) of computer thefts occurred outside traditional business hours.
- ▶ Average total replacement cost of stolen computing devices was \$14,227.27 per device.
- ▶ 72.7% of respondents reported downtime due to computer theft ranging from several days to more than one month.
- ▶ 60.1% of respondent organizations do not have written guidelines on how to safeguard computers from theft.
- ▶ 60.4% of respondent organizations do not provide security guidelines.
- ▶ 76.2% of respondent organizations do not have written guidelines on how to respond to the theft of a computer.
- ▶ 79.3% of respondent organizations do not provide employees with the name and contact information of a specific point of contact when a computing device goes missing.
- ▶ 81.5% of respondent organizations do not conduct periodic security awareness programs on computer theft.
- ▶ 85.4% of respondent organizations do not have a written policy making employees financially responsible for computer theft if security guidelines are not followed.
- ▶ 89.6% of respondent organizations do not have written guidelines on protecting proprietary information on computing devices while traveling.
- ▶ 95% of respondent organizations do not have written guidelines mandating encryption of proprietary information.

---

## Introduction



Computer theft has reached epidemic proportions. Over 1.6 million computers have been stolen in the USA in the last three years alone.

Methods to combat computer theft vary. In addition, because every individual and organization is different, a management approach or business philosophy that works well for one may be ineffective for another, if for no other reason than key people have different approaches to similar problems.

To date, there is little definitive data regarding computer theft, aside from U.S. insurance company theft-loss figures. For example, there is no reliable worldwide data available that narrowly and specifically investigates the chain of events leading up to the theft and the *modus operandi* of the theft. The 2003 BSI Computer Theft Survey, carried out between August 1 and September 6, 2003, is the first survey to make an extensive investigation of the circumstances, demographics, security standards, as well as the logistical and fiscal outcome of computer theft on the individual and organizational user.<sup>1</sup>

The intention of the 2003 BSI Computer Theft Survey is to accumulate reliable data that can be utilized to highlight vulnerabilities and implement security guidelines that safeguard the computer user from theft.

This survey identifies a number of key points for understanding the cost, motivation and consequences of the theft of computing devices.

## The Survey

Brigadoon Software, Inc. conducted the 2003 BSI Computer Theft Survey with the cooperation and participation of KeySurvey ([www.keysurvey.com](http://www.keysurvey.com)). The survey, in its inaugural year, is the first survey of its kind to thoroughly examine all aspects of the theft of computing devices throughout the world.

## The Respondents

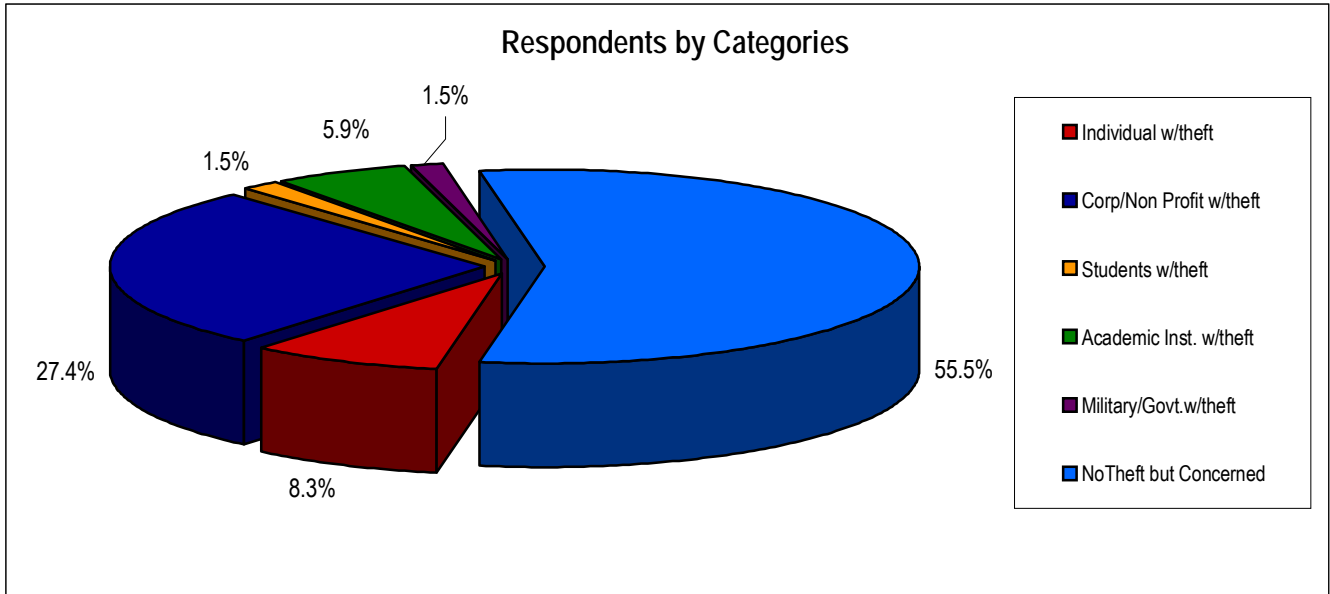
The 2003 BSI Computer Theft Survey, based on the responses of 676 participants throughout the world, had the added benefit of having the respondents reply to the survey questions by sectors, thus allowing for further investigation on a sector-by-sector method.

The survey required the respondents to identify themselves and reply to the survey questions as a member of one of the following sectors:

- Individuals who experienced the theft of computing devices;
- Corporations and non-profit organizations that experienced the theft of computing devices;
- Students who experienced the theft of computing devices;
- Academic institutions that experienced the theft of computing devices;
- Military and government institutions that experienced the theft of computing devices; and
- Individuals who had not experienced the theft of computing devices, but nonetheless are concerned about computer theft.

---

<sup>1</sup> The general term "computer" should be interpreted as "computing devices" unless specifically mentioned. The 2003 BSI Computer Theft Survey looked at the theft of a wide variety of computing devices, including desktops, laptops, workstations, servers, PDAs and even Internet-enabled telephones.



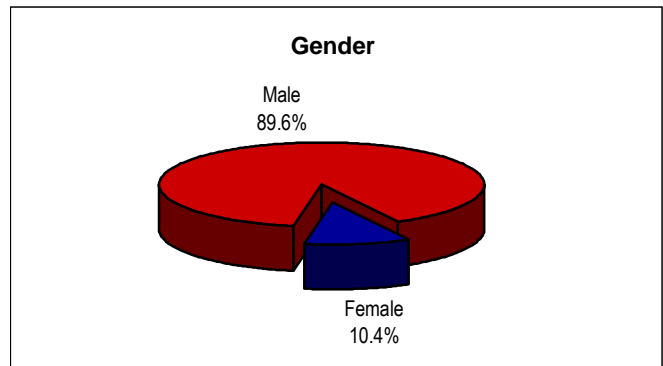
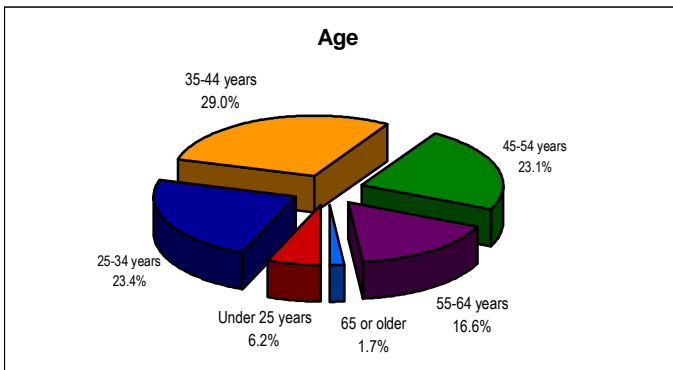
Of the 676 survey respondents, nearly half (44.5%) of those responding either personally experienced the theft of a computing device, or responded on behalf of an organization that experienced the theft of a computing device. (*See graphic, above.*)

Corporate and non-profit organizations head the list of those experiencing computer theft, comprising 27.4% of all survey respondents, following by individuals (8.3%), academic institutions (5.9%) and military/governmental institutions (1.5%).

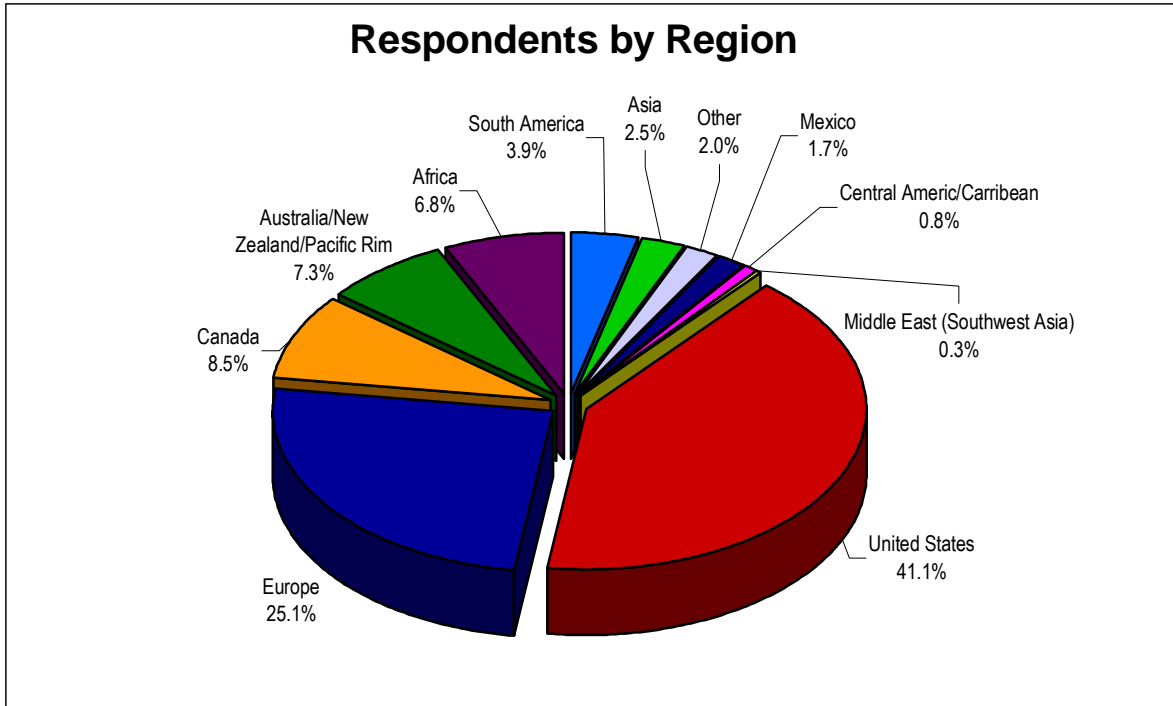
### Age and Gender

The 676 respondents were also asked to provide age and gender demographic information as part of the survey. Male respondents dominated the survey, comprising nearly 9 out of 10 (89.6%) of those who participated.

The age distribution of the survey respondents was essentially equally distributed through those age sectors that reflect the general work force. The 35-44 year age group was the largest group of the 676 respondents (29%), followed by 25-34 age group (23.4%), the 45-54 year age group (23.1%), 55-64 age group (16.6%), under 25 years (6.2%) and 65 and older (1.7%).



## Respondent Geographic Distribution



Respondents from the United States constituted the largest sector, comprising 41.1% of the total 676 respondents, followed by a group comprised primarily of Europe (25.1%), Canada (8.5%), Australia/New Zealand/Pacific Rim (7.3%), and Africa (6.8%).

North Americans comprised 52.1% of the total respondents. It is important to note that 47.9% of the respondents were from regions (outside of North America) where little or no data was available that pertained to computer security in general, and the specific topic of computing device theft.










## Respondents' Job Titles

Top Management was well represented in the survey, with CEOs and Presidents comprising the largest segment of respondents (15.8%). Those who considered themselves self-employed were next with 14.9% of the respondents. <sup>2</sup>










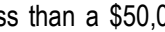
Respondents by current job function	Response Percent
Chief Executive Officer/President	15.8 %
Chief Information/Chief Technology Officer	4.8 %
Chief Financial Officer	1.1 %
Chief Operating Officer	0.8 %
VP/Director of IT/IS/MIS	2.0 %
VP/Director of Purchasing/Procurement	0.3 %
VP/Director of Sales/Marketing	3.7 %
VP/Director of Finance/Accounting	0.3 %
VP/Chief of Operations	1.4 %
Multimedia Director/Manager/Coordinator	0.8 %
IT/IS/MIS Manager	9.3 %
Manager of Sales/Marketing	3.4 %
Systems Manager	3.7 %
Network Manager	0.8 %
Procurement Manager	1.4 %
Network Engineer	1.7 %
Network Administrator	2.5 %
IT Analyst	5.1 %
Manager of Telecommunications	0.6 %
Manager/Director of Network Security	0.8 %
Manager/Director of Security/Risk Management	1.7 %
Crime Prevention Officer/Manager	0.8 %
Military-Security/Investigator	0.6 %
Director of Security/Public Safety	0.8 %
Government-Security/Safety Manager	1.1 %
Education-Faculty	4.8 %
Self Employed	14.4 %
Unemployed-Retired	1.1 %
Student	3.4 %
Other	10.7 %

<sup>2</sup> In some cases, respondents may have had several more choices for answers during the survey. If there were no responses to a choice (*i.e.*, 0% respondents) that choice has been omitted from the display graphics.









61.3% of the respondents belonged to organizations with less than 100 employees.

Respondents by number of employees		Response Percent
Less than 10		33.6 %
10 to 99		27.7 %
100 to 499		13 %
500 to 999		5.9 %
1,000 to 2,499		4 %
2,500 to 4,999		4.2 %
5,000 to 9,999		2.8 %
10,000 or more		4.8 %
Don't Know		4 %

Similar to widely accepted demographic figures, half of the respondents (51.1%) were part of small businesses (organizations with less than \$10 million dollars in annual revenue).

Respondents organization's annual revenue		Response Percent
Less than \$1 million		27.7 %
\$1 million to \$9.9 million		23.4 %
\$10 million to \$49.9 million		7.6 %
\$50 million to \$99.9 million		3.1 %
\$100 million to \$499.9 million		2.8 %
\$500 million to \$999.9 million		1.7 %
\$1 billion to \$4.9 billion		2.8 %
\$5 billion or more		2.3 %
Don't know		15 %
Private Company: Don't reveal revenue		13.6 %

While 55.4% of the respondents' organizations had less than a \$50,000 annual security budget, 5.3% of the respondents' organizations had annual security budgets of \$1,000,000 or more.

Organization's security budget: 2003		Response Percent
Less than \$50,000		55.4 %
\$50,000 to \$299,999		9.9 %
\$300,000 to \$999,999		3.7 %
\$1 million to \$4.9 million		2.5 %
\$5 million to \$9.9 million		1.4 %
\$10 million or more		1.4 %
Don't Know		23.4 %
Other		2.3 %

While the information technology sector comprises the largest sector group (40.1%) the respondents, in general, were well diversified throughout the various sectors.

Respondents organization's primary business	Response Percent
Aerospace & Defense	1.4 %
Automotive & Transport Equipment	0.3 %
Computer Hardware	4.5 %
Computer Software & Services	26.3 %
Consumer Products - Durables	0.6 %
Consumer Products - Non-Durables	0.6 %
Diversified Services	2.8 %
Drugs	0.6 %
Electronics & Miscellaneous Technology	0.8 %
Energy	0.3 %
Financial Services	2.3 %
Food, Beverage & Tobacco	0.6 %
Health Products & Services	3.4 %
Insurance	0.8 %
Legal	1.4 %
Leisure	1.4 %
Manufacturing	2.3 %
Materials & Construction	0.8 %
Media	4.2 %
Real Estate	1.1 %
Retail	1.1 %
Specialty Retail	1.1 %
Telecommunications	4.5 %
Utilities	0.6 %
VAR/Distributor/IT Consultant/System Integrator	9.3 %
Government-National	1.1 %
Government-State/Provincial	0.6 %
Government-Local	2 %
Government-Military	0.8 %
Education (K-12)	2.5 %
Education (Higher-Ed)	9.0 %
Other	10.7 %

# Anatomy of Computer Theft

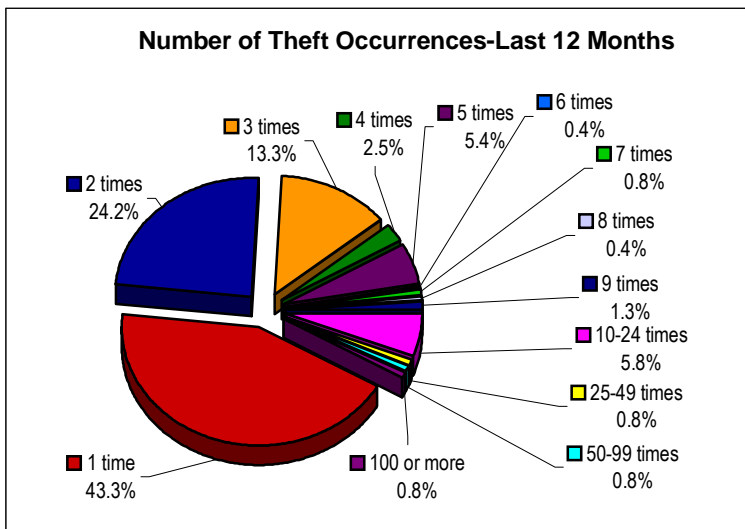
The main goal of this survey was to examine, in detail, the *modus operandi* of computer theft. With that in mind, this section looks at computer theft through “who, what, when, where, how and why” criteria.

## Stolen: How Many Incidents

We asked respondents who identified themselves as having experienced computer theft,

*“How many times has your organization been the victim of computing device(s) theft in the last 12 months?”*

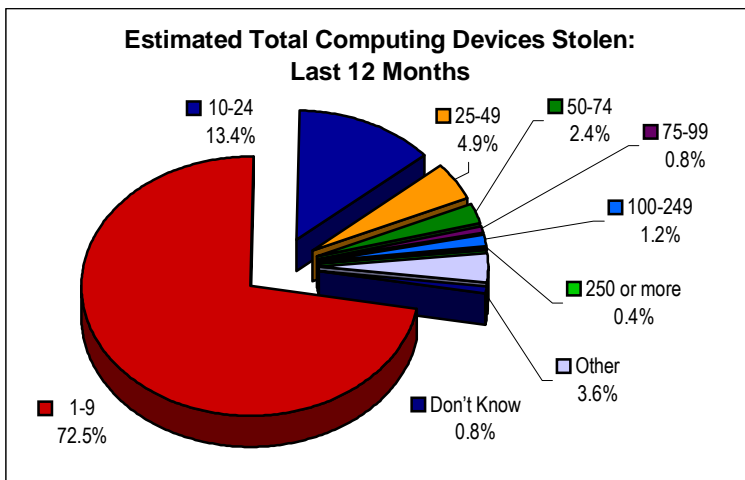
That is, respondents were asked how many separate incidences of theft they experienced during the previous 12-month period.



While the majority of respondents had only 1-2 theft occurrences (67.5% total), 7.4% of the respondents' institutions experienced 10 or more separate theft occurrences in the last 12 months.

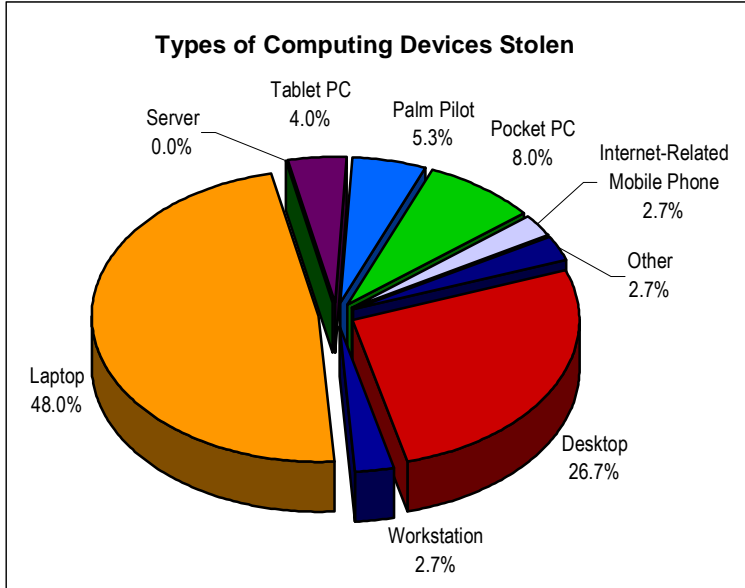
## How Many Stolen

We also asked respondents who identified themselves as having experienced computer theft, *“What would you estimate is the total [number] of computing devices(s) stolen from your institution in the last 12 months?”*



While nearly three-quarters (72.5%) of the respondents had 1-9 computers stolen in the last 12 months, nearly 1 in 10 (9.7%) of the respondents had 25 or more computing devices stolen during that same period.

## What Was Stolen

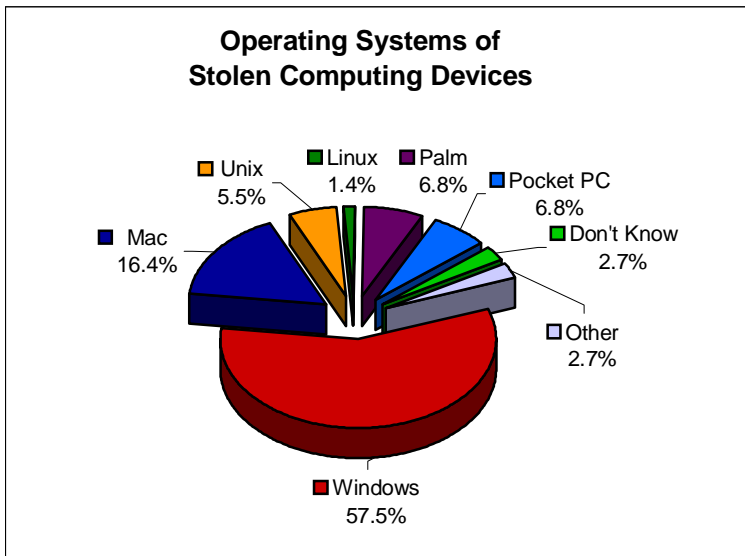


Not surprising, laptops head the list of stolen computing devices by those respondents who reported computer theft. Laptops comprised nearly half (48%) of those devices reported as stolen, followed by desktop computers (26.7%).

In addition, personal digital assistants (PDAs) comprised a considerable segment (13.3%) of the stolen devices. Respondents reported that PDAs using the Pocket PC operating system headed the list of PDAs (8%) stolen, followed by Palm-based PDAs (5.3%).

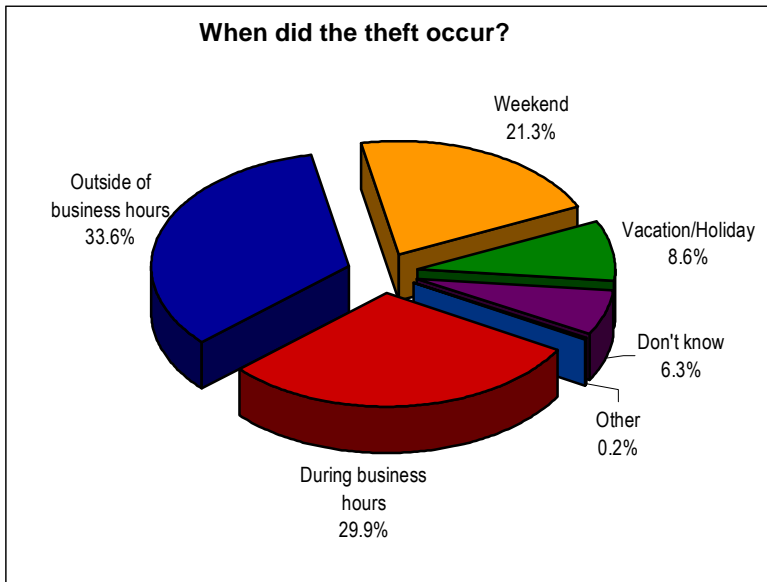
Also of note is that Tablet PCs accounted for 4% of the stolen computing devices.

## Operating Systems of Stolen Computers



While Windows was the predominant operating system on the stolen computing devices, the survey showed a higher percentage of theft for other operating systems, Macintosh (16.4%), and the PDA operating systems (Palm and Pocket PC-6.8% each) than would be indicated from generally accepted market-share industry figures.

## When It Was Stolen



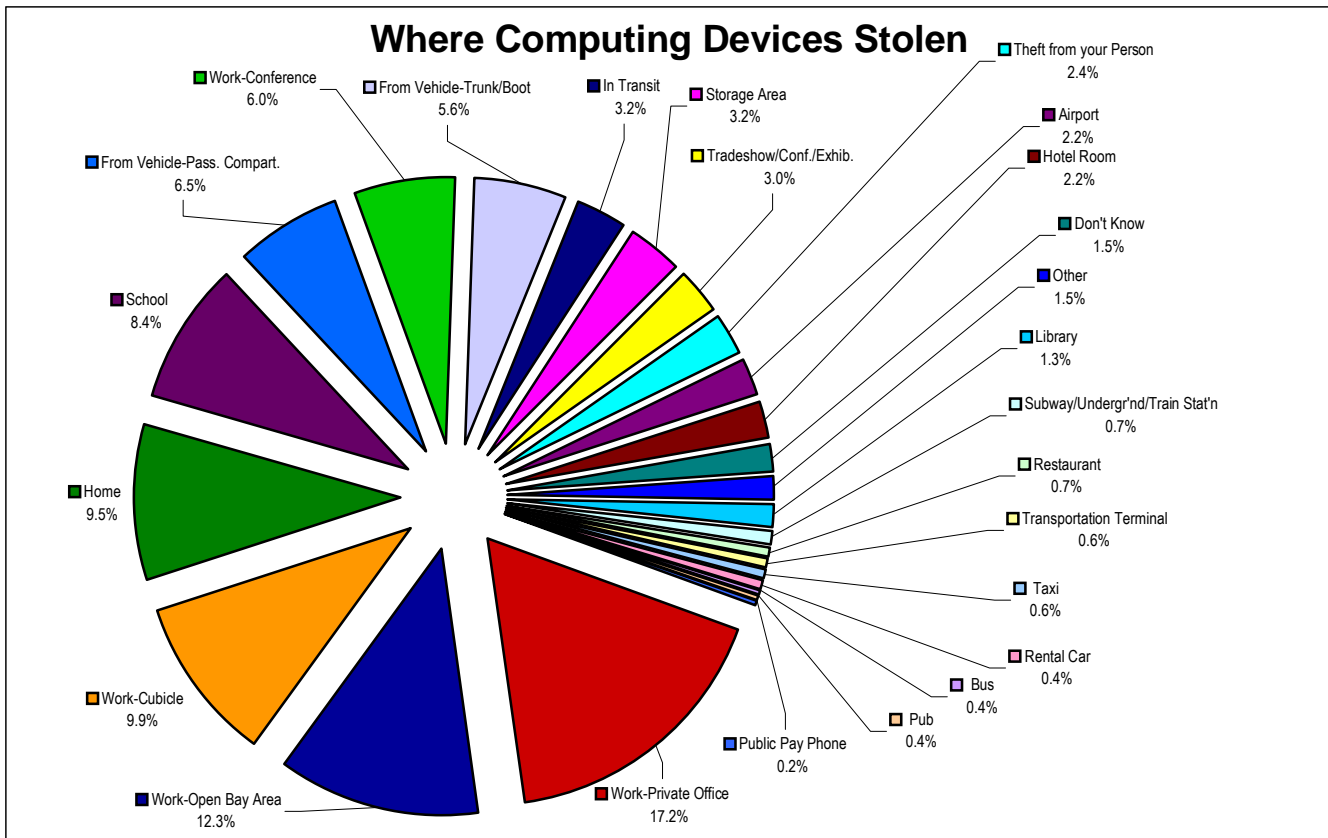
The "time of theft" of computing devices follows expected patterns: 63.5% of the thefts occurred outside traditional business hours.

- Outside of business hours (33.6%)
- Weekends (21.3%)
- Vacation/Holiday (8.6%)

Nonetheless, nearly one-third (29.9%) of the thefts occurred during normal business hours.

## Where It Was Stolen

While expected venues (at work-combined 28.2%; at home-9.5%; at school-8.4%) accounted for 46.1% of the locations where computing devices were stolen, over half (53.9%) of the thefts occurred in mobility-related venues where traditional methods of computer anti-theft security (cables and locks, computer trolleys, metal enclosures, etc.) would have little or no use or effectiveness.



## Where It Was Stolen: Stationary Locations

The survey then took a detailed look at methods of entry where computing devices were stolen from stationary (*i.e.*, non-mobile) locations.

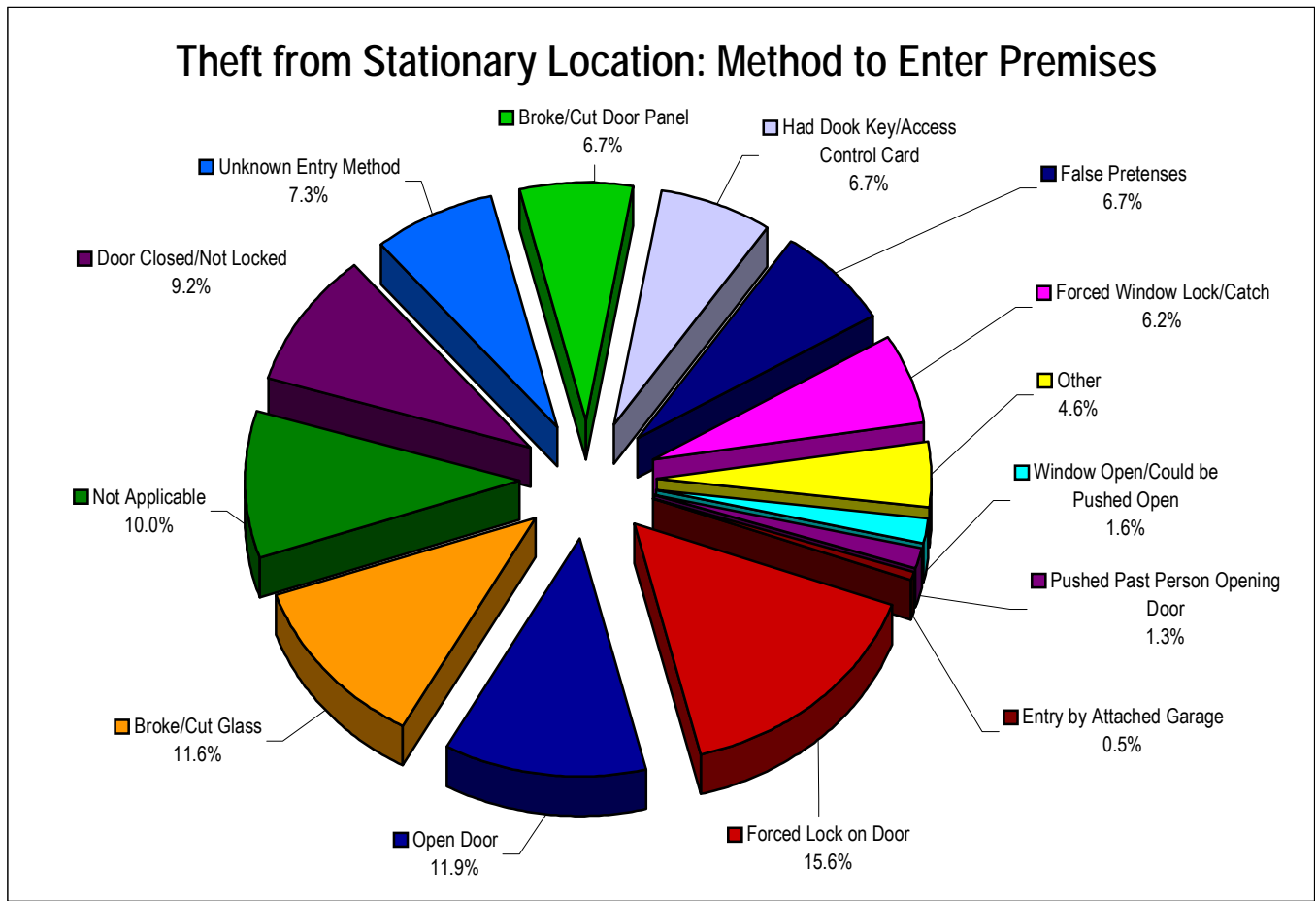
The survey asked the following question:

*If your computing device(s) were stolen from a stationary location(s), what methods were used to enter the premises to facilitate the theft(s)?*

Respondents were then given a choice of 14 different methods from which to choose that covered standard theft and burglary techniques.

While the information provided by respondents is self-evident (see graph below), it is interesting to note that nearly one-quarter (22.7%) of the perpetrators entered the premises unhindered by in-place security. Those means were the following:

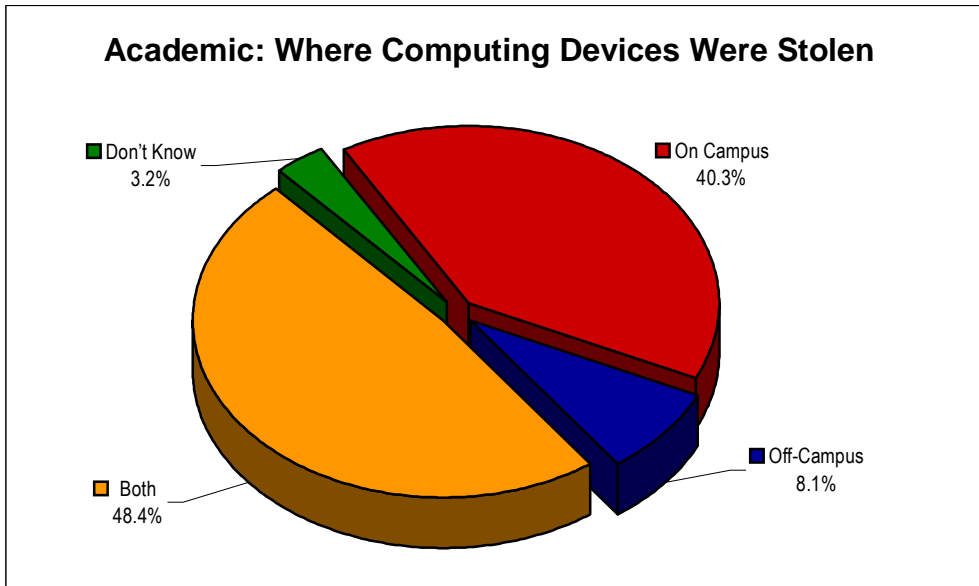
- Open Door 11.9%
- Door Closed/Not Locked 9.2%
- Window Open/Could be Pushed Open 1.6%



Where It Was Stolen: Academic Sector

As part of the survey, we asked students and members of academic organizations that experienced the theft of a computing device questions specific to the academic sector.

Survey respondents reported that the computing devices were primarily stolen on-campus.



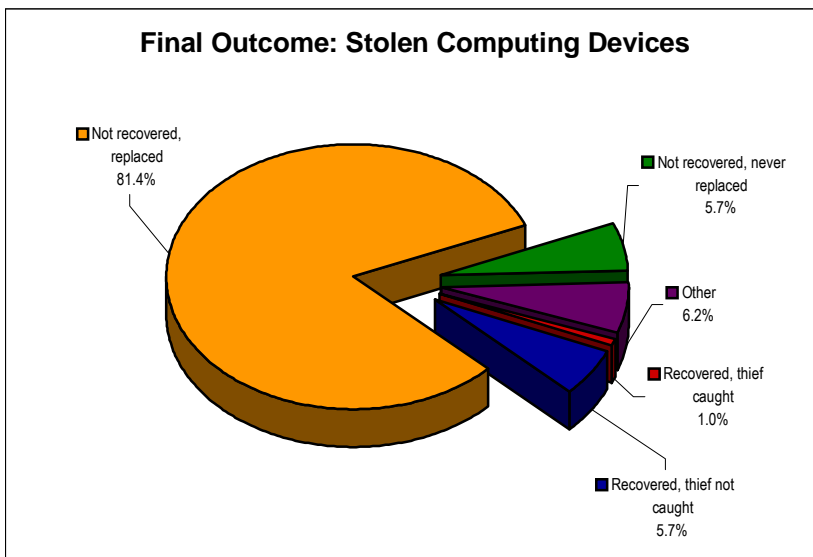
The survey then asked respondents to provide specific information as to *where* on campus the computing devices were stolen. By an overwhelming margin, 54.8 % of all academic respondents that replied to this question indicated that the computing devices were predominantly stolen from school classrooms.

Where on-campus was the computing device stolen? (Check all that apply.)	
	Percentage
Classroom	54.8%
Administrative Offices	29.0%
Laboratory	25.8%
Not Applicable	16.1%
Storage Area	12.9%
Don't Know	9.7%
Dormitory Residence	6.5%
Student Center	6.5%
Library	6.5%
From Vehicle-Pass. Compartment	6.5%
Theft from a Person	6.5%
Other	6.5%
Off Campus Residence	3.2%
From Vehicle-Trunk/Boot	3.2%
In Transit	3.2%
Locker	3.2%

## Why It Was Stolen

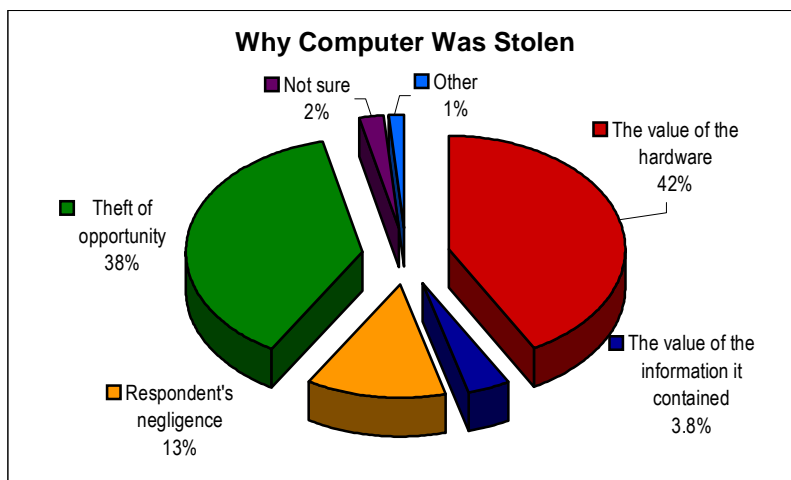
We asked respondents what was the final outcome of the theft incidents they experienced. Not surprisingly, almost 90% (87.1%) of the respondents said that the stolen computing device was never recovered.

- 81.4% of the respondents indicated that the stolen computing device was never recovered and was replaced
- 5.7% of the respondents indicated that the stolen computing device was never recovered and was never replaced



Of note is that only 1% of the respondents indicated that the stolen computing device was recovered and the thief was caught. It is therefore reasonable to conclude that in 99% of the cases, the thief was not caught, thereby remaining free to continue to perpetrate computer theft crimes.

In addition, we asked respondents to give us their opinions on what factors came into play on *why* their computing devices were stolen. While not a truly scientific indicator (that would require a survey of the perpetrators, not the victims), it nonetheless provides some sense of motivation from those who are intimate with the facts surrounding the theft of computing devices.



Heading the list of indicators:

- The value of the hardware – 42%
- Theft of opportunity – 38%
- Victim Negligence – 13%
- The value of the information it contained – 3.8%

While it is interesting to note that only 3.8% of the respondents indicated that the information on the stolen computing device was the motivation for the theft (which may be skewed by the volume of individual and academic respondents-*i.e.* non-commercial/non-governmental respondents), the numerous instances where proprietary information worth substantial amounts (\$1 million or more) may indicate that a “quality not quantity” scenario exists.

# The Cost of Computer Theft

The cost of replacing stolen hardware is just the initial loss factor to the assessment of the actual cost of computer theft. In order to accurately estimate the loss, the loss calculation must account for all of the following factors:

1. Cost of the computer hardware;
2. Value of data and work product contained on computer;
3. Cost of non-productive time to replace, re-install programs and re-configure the replacement machine;
4. Reduced productivity until computer replacement is completed; and
5. The possibility of confidential information getting into the wrong hands.

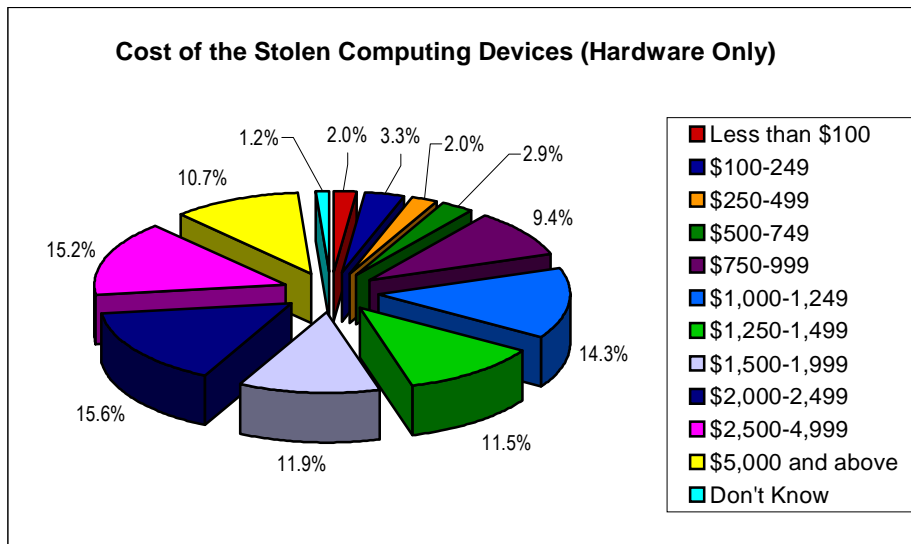
The 2003 BSI Computer Theft Survey sought to quantify these aspects of the cost of computer theft within the survey.

## Cost of the Computer

The respondents who experienced computer theft were asked the following question to quantify the value of the stolen hardware only:

*What was the average cost of the computing device(s) stolen from you/your organization (hardware only)?*

Respondents were given a range of amounts (in USD) from which to reply (see graph below).<sup>3</sup>

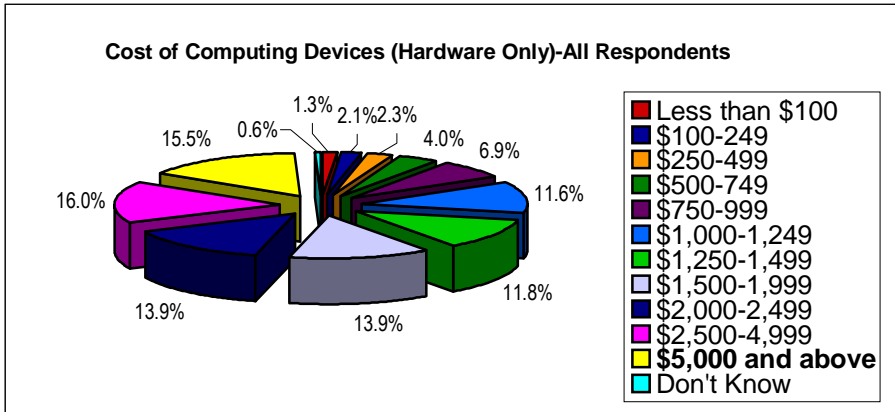


Nearly 80% of the respondents indicated that the cost of the stolen computing device hardware was \$1,000 or greater.

- \$1,000-1,249: 14.3%
- \$1,250-1,499: 11.5%
- \$1,500-1,999: 11.9%
- \$2,000-2,499: 15.6%
- \$2,500-4,999: 15.2%
- \$5,000 plus: 10.7%

<sup>3</sup> Respondents were asked to submit responses calculated in U.S. Dollars, and were provided with a currency converter hyperlink to utilize once they made their calculation in their native currency.

The survey also asked those respondents who had not experienced computer theft to also estimate the hardware-only replacement cost of their own computing devices. When the responses to the average hardware replacement cost all survey respondents (including those who had not experienced computer theft) is included, the estimated average replacement cost of computing devices list at \$5,000 or greater jumps by nearly 5% (4.8%).



Average Hardware Cost

A calculation of the average hardware cost of the stolen computing devices was estimated at approximately \$2,404.86 per computing device stolen. When all respondents' data (including those who did not experience computing device theft, but were also asked to estimate the hardware cost of their device) is included, the approximate cost is \$2,640.29 per computing device.

It is important to note that this calculation included a number of devices that are, by their very nature (*i.e.* PDAs and mobile Internet telephones) cost well under \$1,000. This may, in fact, artificially lower the average cost below realistic and accurate amounts.

Hardware replacement cost of \$5,000 and above:

- Stolen Computing Devices: 10.7%

Compared to:

- All Computing Devices: 15.5% (see graphic, right)

## Total Replacement Cost of the Computer Replacement

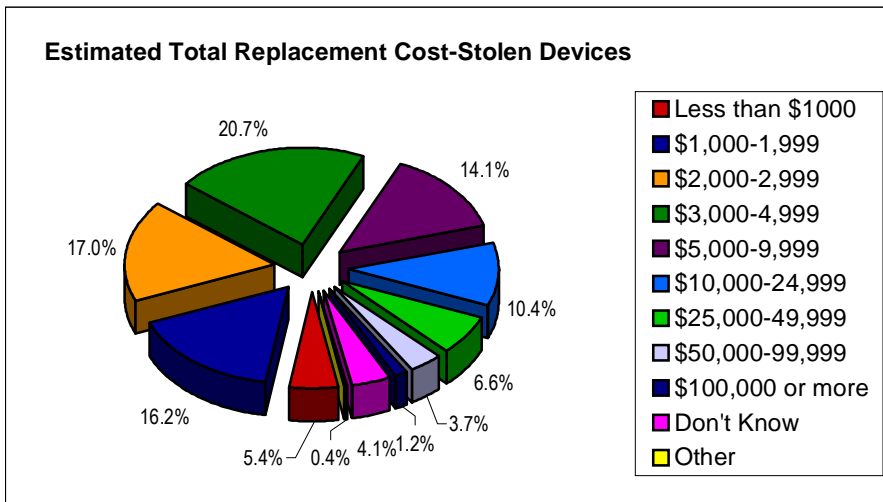
Then respondents who experienced computer theft were asked the following question to quantify the total replacement cost of the stolen computing device(s):

*What is your estimate of the average replacement cost of your organization' stolen computing device(s)?*

Respondents were asked to include in their calculation the following criteria:

- The cost of the hardware
- All installed software
- Labor to setup a new computing device
- Estimated value of downtime
- Lost productivity
- Income from lost sales and any legal ramifications; and
- Investigation fees associate with the loss of the computing device(s)

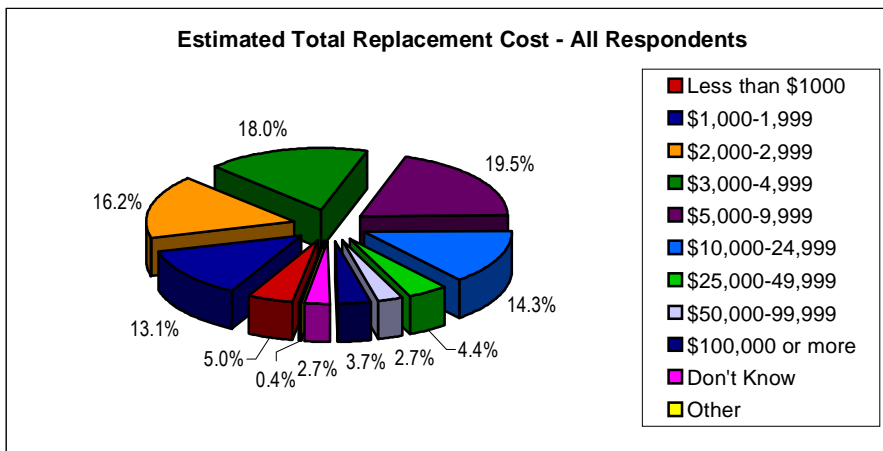
Respondents were then given a range of amounts from which to reply. (See graph below)



The top responses were the following:

- \$1,000-1,999: 16.2%
- \$2,000-2,999: 17.0%
- \$3,000-4,999: 20.7%
- \$5,000-9,999: 14.1%
- \$10,000-24,999: 10.4%
- \$25,000-49,999: 6.6%

When the responses to the average total replacement cost estimates of all survey respondents (including those who had not experienced computer theft) are included, the estimated average replacement cost of computing devices listed at the \$5,000-9,999 range and the \$10,000-24,999 range jumps by 4.4% and 4.1% respectively.



Replacement Cost Increases (all respondents):

- \$5,000-9,999: +4.4% (14.1%-19.5%)
- \$10,000-24,999: +4.1% (10.4%-14.3%)

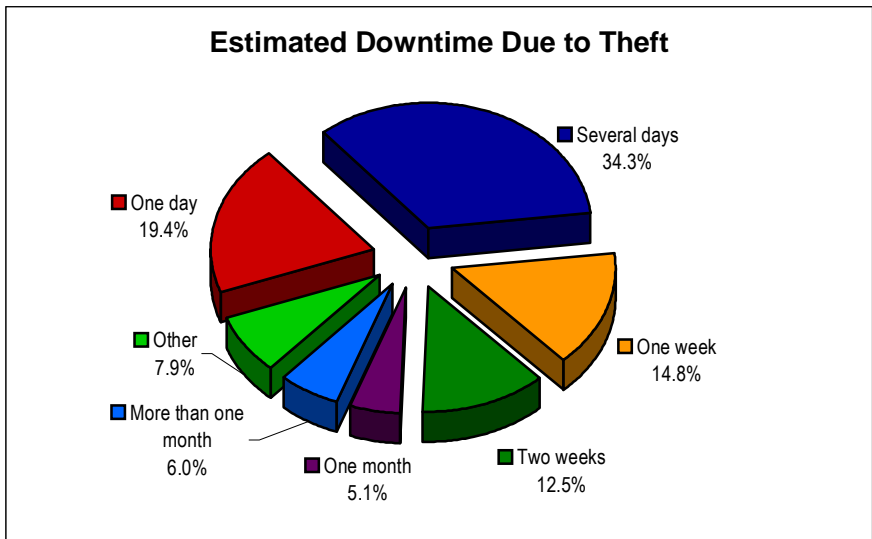
### Total Replacement Cost: Averages

A calculation of the average total replacement cost of the stolen computing devices was estimated at approximately \$14,227.27 per computing device stolen. When all respondents' data (including those who did not experience computing device theft, but estimated the hardware cost of their device) is included, the approximate cost is \$15,834.95 per computing device.

It is important to note that this calculation included a number of devices that, by their very nature (*i.e.* PDAs and mobile Internet telephones) cost well under \$1,000. In addition, while PDAs with greater functionality are at the vanguard of next generation of mobile computing, they do not yet enjoy widespread deployment. These factors may therefore artificially lower the average cost below actual present-day numbers.

### Cost of Computer Theft: Downtime

Another component of the cost of computer theft is the loss of productivity due to the down time experienced by the primary user of the stolen computing device, as well as loss of productivity of any additional individuals that must now divert their attention to the restoration process.

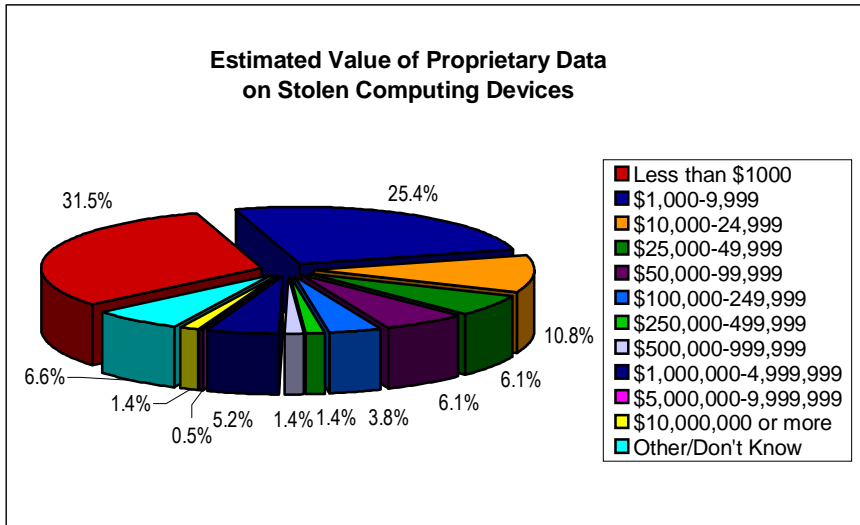


72.7% of survey respondents that experienced computer theft indicate that the downtime due to the theft being several days to more than one month.

- Several days – 34.3%
- One week – 14.8%
- Two weeks – 12.5%
- One month – 5.1%
- More than one month – 6.0%

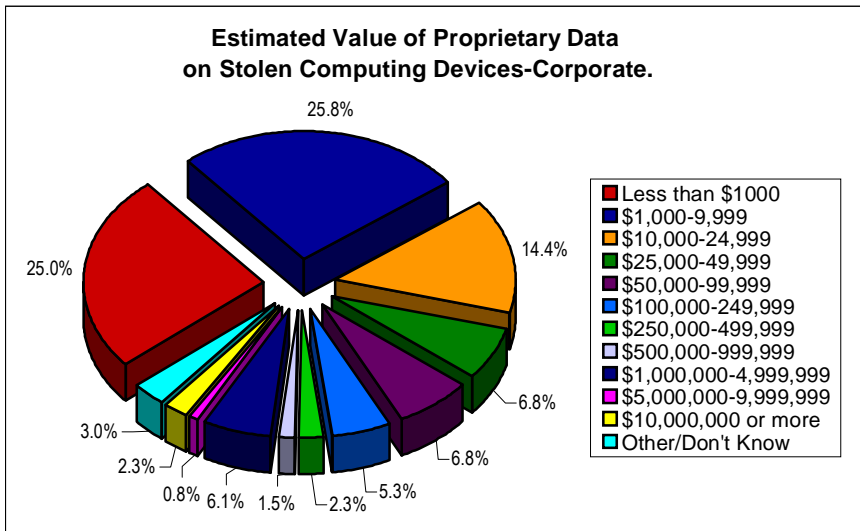
## The “Real” Cost of Computer Theft: Loss of Proprietary Data

The final component of the cost of computer theft is the loss and exposure of proprietary data contained on the stolen computing device. For most commercial and research entities, whether they be private or public sector, the possibility of confidential information getting into the wrong hands is a problem of paramount importance.



The combined data indicates that 67.7% of all survey respondents that experienced theft estimated that the value of the proprietary data on their stolen computing devices at \$25,000 or less.

However, looking at the responses of corporate sector respondents show that estimated value of the proprietary data on stolen computing devices raises appreciably.



Nearly one out of ten (9.2%) of the corporate respondents indicated that the stolen computing device contained proprietary data with \$1,000,000 or more on it, with 2.3% of the corporate respondents valuing the proprietary data at \$10,000,000 or more.

### Average Value of Proprietary Data

A calculation of the average value of proprietary data on stolen computing devices was estimated at an astronomical \$690,759.61 per computing device stolen. When all respondents' data (including those who did not experience computing device theft, but estimated the value of their proprietary data) is included, the approximate cost is an equally astounding \$629,021.64 per computing device.

Clearly, the average is weighed heavily by the substantial numbers in the highest amount estimate brackets. The top brackets had 9.2% of the total respondents who estimated their proprietary data at \$1,000,000 or more (including 2.3% at over \$10,000,000).

However it should be noted that, even if all estimates \$1,000,000 USD or more are eliminated from the calculation, the average estimated value of the proprietary data is still \$73,667.38 per stolen computer.

### What Proprietary Data- Stolen Computers

Those respondents who experienced computing device theft were asked to consider various types of proprietary data present on the computing devices at the time of loss. The respondents were then asked to indicate all of the types of proprietary data that was on the computing device at the time of theft (*i.e.*, “check all that apply”). The table below indicates what percentage of each proprietary data category the total respondents to this question (209) had on the stolen computing device.

<b>Please check if the stolen computing device(s) contained any of the following information. (Check all that apply)</b>		
No. of Respondents: 209	Total	Percent
Project Assignments	190	90.9%
Work Schedules	186	89.0%
Financial Projections	112	53.6%
Sales Statistics	109	52.2%
Research Plans	96	45.9%
Product Designs	93	44.5%
Contract Bids	93	44.5%
Customer/Mailing Lists	89	42.6%
Personnel Records	89	42.6%
Profit Margins	89	42.6%
Proposals, Contract and Bids	86	41.1%
Computer Generated/Stored Information	79	37.8%
Material Costs	73	34.9%
Marketing Strategies	57	27.3%
Vendor Lists	53	25.4%
None	43	20.6%
Financial and Legal Documentation	42	20.1%
Computer Codes	37	17.7%
Buying and Selling Programs	28	13.4%
Trade Secrets	24	11.5%
Workplace Capacities/Expansion	24	11.5%
Manufacturing Techniques	23	5.3%
Student Records	20	9.6%
Other	14	6.7%
Medical Records	11	5.3%
Litigation Tactics	11	5.3%
Negotiations w/Labor or Unions	10	4.8%
Labor Negotiating Positions	6	2.9%
Take-over Strategies	5	2.4%

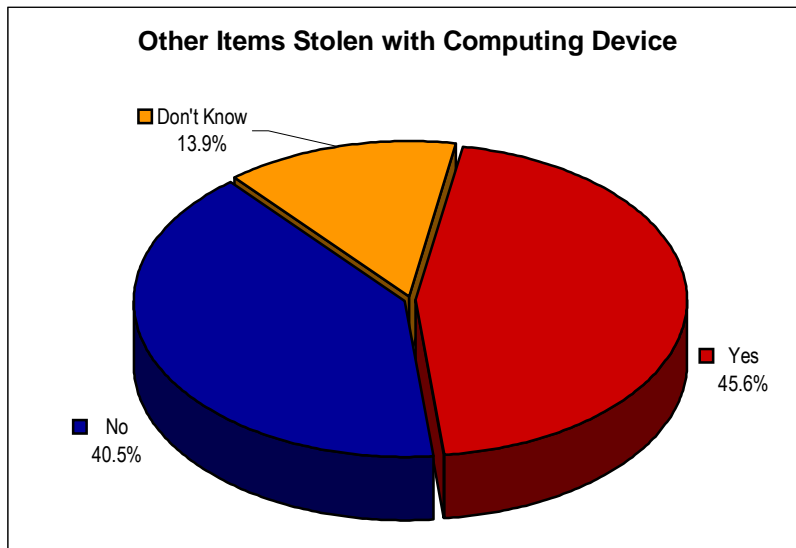
**What Proprietary Data- All Respondents' Computers**

As part of the survey, those respondents who had not experienced computer theft were also asked to assess the proprietary data on their computing devices. The table below indicates what percentage of each proprietary data category the combined theft (209) and non-theft respondents (269) to this question had on their computing devices.

Please check if your computing device(s) contains any of the following information - All Respondents. (Check all that apply)		
No. of Respondents: 478	Total	Percent
Personnel Records	252	52.7%
Computer Generated/Stored Information	251	52.5%
Customer/Mailing Lists	248	51.9%
Proposals, Contract and Bids	239	50.0%
Project Assignments	190	39.7%
Work Schedules	186	38.9%
Vendor Lists	173	36.2%
Marketing Strategies	155	32.4%
Financial and Legal Documentation	146	30.5%
Computer Codes	122	25.5%
Financial Projections	112	23.4%
Sales Statistics	109	22.8%
Research Plans	96	20.1%
Product Designs	93	19.5%
Contract Bids	93	19.5%
Profit Margins	89	18.6%
Trade Secrets	86	18.0%
Buying and Selling Programs	77	16.1%
Material Costs	73	15.3%
Student Records	53	11.1%
None	43	9.0%
Other	42	8.8%
Medical Records	40	8.4%
Negotiations w/Labor or Unions	32	6.7%
Workplace Capacities/Expansion	24	5.0%
Manufacturing Techniques	23	4.8%
Litigation Tactics	11	2.3%
Take-over Strategies	10	2.1%
Labor Negotiating Positions	6	1.3%

## What Else Was Stolen

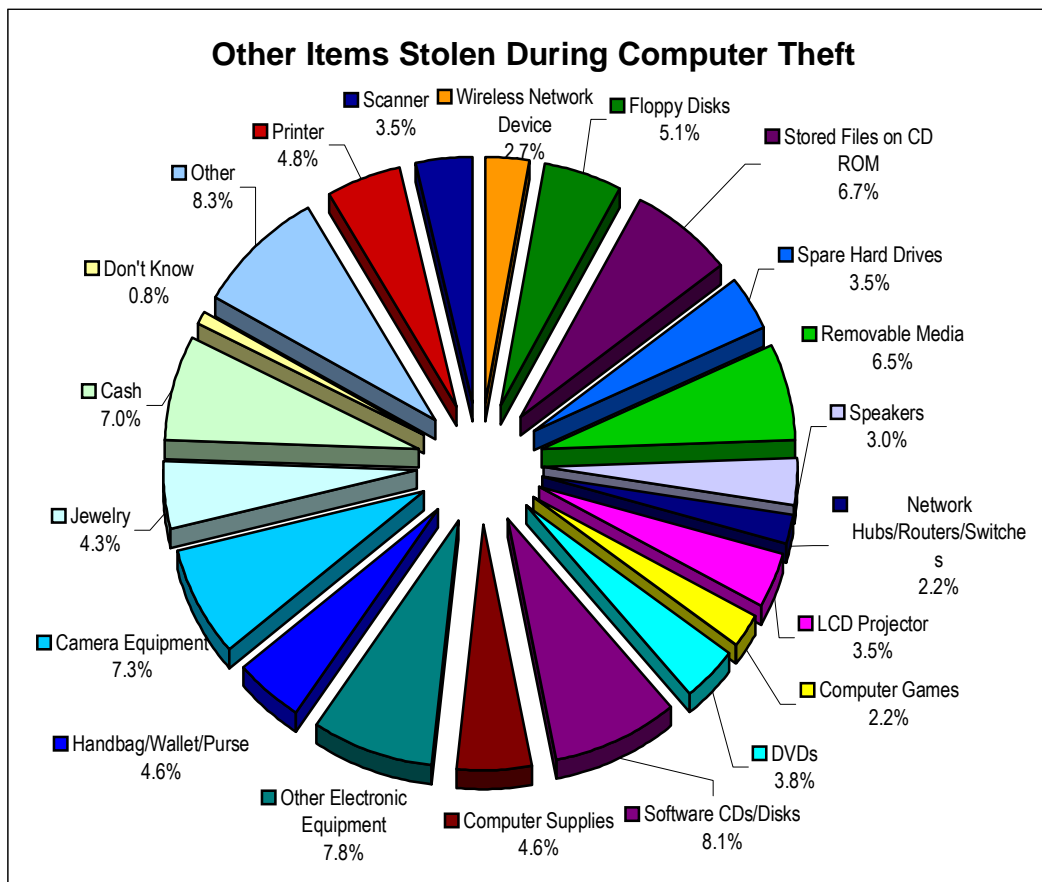
The 2003 BSI Computer Theft Survey also investigated what other items (if any) were part of the computer theft incident.



45.6% of the respondents that had experienced computer theft indicated that other items were stolen during the computer theft.

40.5% indicated no additional items, and 13.9% did not know.

The survey then specifically investigated exactly what the other items stolen during the computer theft were. Respondents were provided with a large selection of items and were allowed to select all items that applied.



45.6% of survey respondents that experienced computer theft report other items were stolen at the time of the computer, with removable media (including spare disks, stored files on CDs, removable and spare hard drives) accounting for 21.8% of the additional stolen items.

## Computer Theft: Countermeasures

The 2003 BSI Computer Theft Survey explored the issue of security and counter-measures specifically related to computer theft. Respondents that experienced computer theft were asked what security precautions (if any) were in place at the time they experienced the theft of the stolen computing devices.

Of those experiencing computer theft, 92.7% of the respondents used logon passwords, and 70% recorded and stored the make, model and serial number of the computing device in a safe area. However, almost one-quarter (23.3%) of the respondents used no security precautions to safeguard their stolen computing device.

<b>What, if any, of the following security precautions did your organization use to safeguard your stolen computing device(s)? Check all that apply.</b>		
	<b>Total</b>	<b>Percent</b>
No. of Respondents: 150		
Logon Password	139	92.7%
Make, model and serial number recorded and stored in a safe area	105	70.0%
Password Protected Screensaver	64	42.7%
Engraved/ID Sticker/ID Plate with ownership information	42	28.0%
BIOS Password	41	27.3%
None	35	23.3%
Cable and Lock	33	22.0%
Locked Enclosure/Laptop Safe	20	13.3%
Encryption of Proprietary Data	18	12.0%
Authentication Token	14	9.3%
Other	13	8.7%
Motion Sensor	11	7.3%
Tracking and Location Software	9	6.0%
Disk Drive Lock	8	5.3%
Biometric Device	3	2.0%

When the answers of all respondents are included in the calculation, no more than one-third of the respondents utilize other security precautions besides logon passwords and storing make, model and serial number information.

**What, if any, of the following security precautions did your organization use to safeguard your computing device(s)-All Respondents? Check all that apply.**

No. of Respondents: 411	All Total	All Percent
Logon Password	365	88.8%
Make, model and serial number recorded and stored in a safe area	258	62.8%
Password Protected Screensaver	153	37.2%
BIOS Password	109	26.5%
Cable and Lock	102	24.8%
Encryption of Proprietary Data	87	21.2%
Engraved/ID Sticker/ID Plate with ownership information	83	20.2%
Tracking and Location Software	67	16.3%
None	54	13.1%
Motion Sensor	45	10.9%
Locked Enclosure/Laptop Safe	39	9.5%
Disk Drive Lock	36	8.8%
Authentication Token	35	8.5%
Other	33	8.0%
Biometric Device	19	4.6%

**Countermeasures Utilized After Theft: Increased Usage of Tracking/Location Software**

The survey asked those who had experienced computer theft to indicate what anti-theft/security actions were taken after the theft of their computing device(s), and the question mirrors the security question about pre-theft protocols.

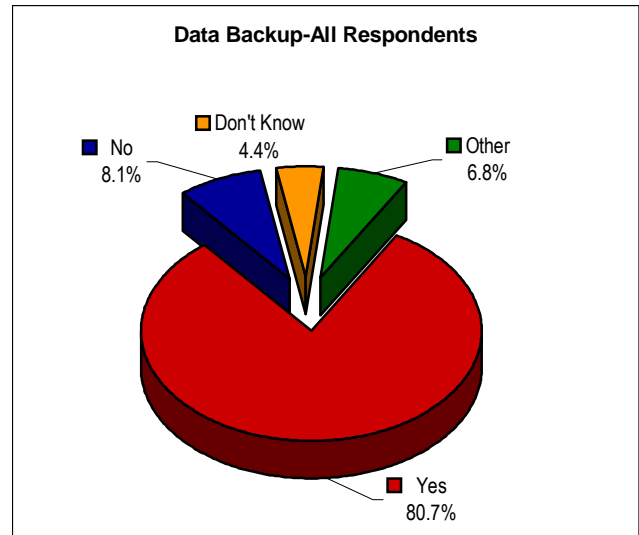
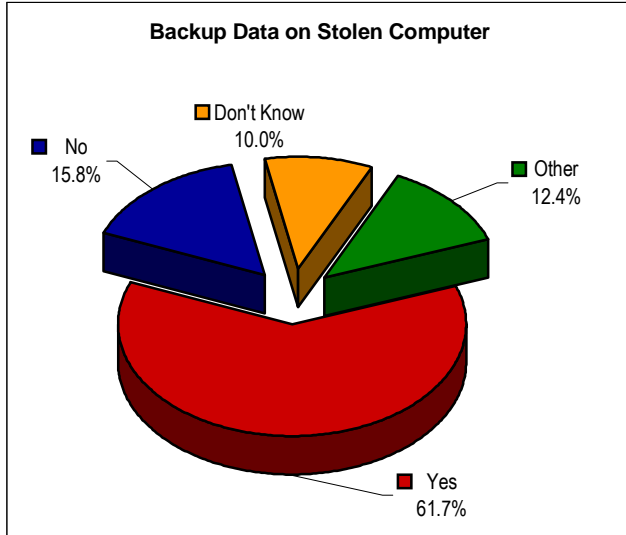
In comparing the responses, most categories either stayed level or had slight downturns. However, one category, "Tracking and Location Software" enjoyed a substantial increase. The use of tracking and location software showed a 200%+ increase in usage by respondents who had experienced computer theft (from 6.0% to 18.4%).

**Since you have already experienced the theft of a computing device(s), what, if any, of the following security measures do you currently use to protect your new computing device(s)? Check all that apply.**

	Percent
Logon Password	69.7%
Make, model and serial number recorded and stored in a safe area	56.2%
Password Protected Screensaver	35.7%
Cable and Lock	35.7%
BIOS Password	30.3%
Engraved/ID Sticker/ID Plate with ownership information	26.5%
Encryption of Proprietary Data	22.7%
Tracking and Location Software	18.4%
Locked Enclosure/Laptop Safe	14.1%
Motion Sensor	13.0%
Authentication Token	11.4%
Disk Drive Lock	10.3%
Other	7.6%
None	5.9%
Biometric Device	4.9%

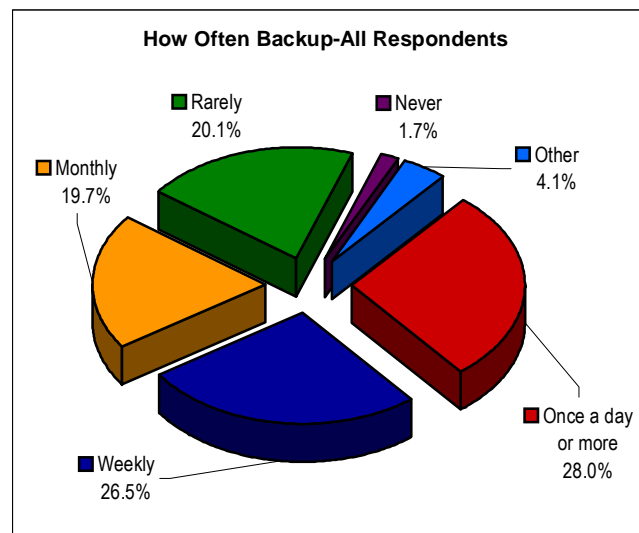
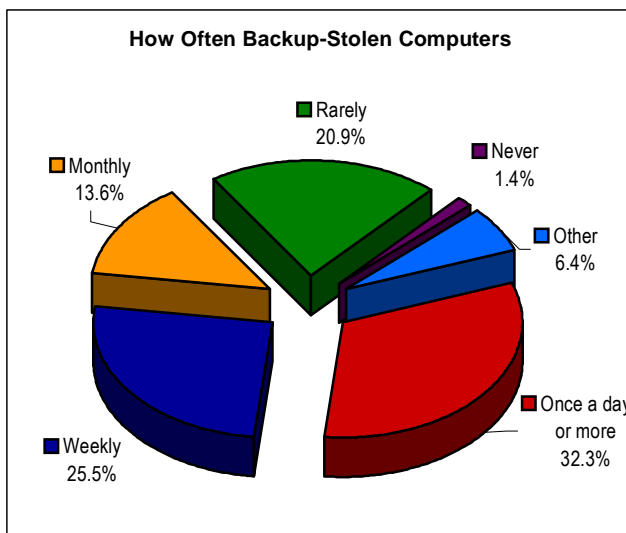
## Data Backup

Respondents were asked whether or not the data on their computers was backed up. Of those who reported stolen computers, 61.7% indicated that they did back up data, while 80.7% of all respondents (including those that had not experienced theft of a computing device) backed up their data.



## Backup: How Often

When respondents were asked the frequency of their backup activities, 61.4% admitted to backing up the data on their stolen computer once per week or less. When all survey respondents are included, an even greater percentage (68%) of all respondents back up their data once per week or less.



## Organizations: Security Guidelines

The 2003 BSI Computer Theft Survey investigated organizational security structure as it pertains to computer theft. Institutional respondents that experienced computer theft (*i.e.*, corporate, non-profit, academic and government/military sectors) were asked about the status of their security guidelines program, as it specifically related to computer theft. Each respondent could check as many of the choices as applied to their institution.

While nearly 41% of the respondents (40.9%) indicated that their institutions had written guidelines on how to safeguard computers from theft, nearly the same amount (39.6%) indicated that they had no computer theft security guidelines in place at all.

23.8% of the respondents indicated that their institution had written guidelines on how to respond to the theft of a computer; 20.7% said that employees have a specific point of contact for computer theft.

<b>What, if any, of the following security guidelines does your institution provide to employees? (Check all that apply)</b>	
	<b>Percent</b>
Written guidelines on how to safeguard computers from theft	40.9%
No security guidelines provided	39.6%
Written guidelines on how to respond to the theft of a computer	23.8%
Employees provided the name and contact information of a specific point of contact when a computing device goes missing	20.7%
Periodic security awareness programs on computer theft	19.5%
Written policy making employees financially responsible for computer theft if security guidelines not followed	14.6%
Written guidelines regarding proprietary information on computing devices while traveling	10.4%
Written guidelines mandating encryption of proprietary information	5.0%
Other	1.2%

---

# Conclusions and Recommendations

## Conclusions

There are two types of computer owners in the world today. Those who have experienced the theft of a computing device and those who have not yet become a victim. Computing devices have become repositories for our most guarded secrets.

The 2003 BSI Computer Theft Survey confirms the suspicions of computer and security experts as to the epidemic of computer theft sweeping the world today. No segment of industry or academia is immune. Individuals also need to take heed, for the survey shows that they are also a target.

Nearly half (44.5%) of the respondents have been victims of computer theft in the last 12 months. Nearly half (46.7%) have been the victim of computer theft on multiple occasions in the last 12 months. Some lessons are learned the hard way. Almost three quarters (72.5%) of the respondents suffered the theft of between 1 and 9 computers in the last 12 months; nearly 1 in 10 (9.7%) had more than 25 computers stolen in the last 12 months.

53% of computer theft occurred while the respondent was mobile (moving about) rendering cables, locks and enclosures virtually useless. Nearly two-thirds (63.5%) of computer thefts occurred outside traditional business hours. Laptops comprised nearly half (48%) of those devices reported stolen, followed by desktop computers (26.7%) and PDAs (13.3%).

68% of respondents report they only back-up data weekly, monthly, rarely or never – making the theft of a computing device a serious event that results in the permanent loss of data. Perhaps that is why 72.7% of respondents reported downtime due to computer theft ranging from several days to more than one month and the average total replacement cost of stolen computing devices was \$14,227.27 per device.

67.7% of respondents report the estimated value of proprietary data on their stolen computing device at \$25,000 or less; 9.2% estimated the value at \$1,000,000 or more and 2.3% estimated the value at more than \$10,000,000. The value of proprietary data on respondents' stolen computers averaged a whopping \$690,759.61 per stolen computer. An alarming number (88%) of respondents did not encrypt the proprietary data on their stolen computing device. The end result is that a lot of trade secrets and important (maybe irretrievable) data is lost every year.

45.6% of respondents report other items were stolen at the time of the computer theft, with recordable media (including floppy disks, stored files on CDs, removable media and spare hard drives) accounting for 21.8 % of the additional stolen items. How many on these items contained more proprietary data?

92.7% of respondents use only a log-on password to protect their computer; 70% recorded and stored the make, model and serial number of the computer in case of theft. No other security measures are used in any appreciable manner.

Almost one quarter (23.3%) used no security precautions at all to safeguard their computing device from theft. It is therefore not surprising that 99% of survey respondents that experienced computer theft report the thief was never caught.

Organizations have not adequately addressed the computer theft issue, based on the following data:

- 60.1% of respondent organizations do not have written guidelines on how to safeguard computers from theft.
- 60.4% of respondent organizations do not provide security guidelines.
- 76.2% of respondent organizations do not have written guidelines on how to respond to the theft of a computer.

- 
- 79.3% of respondent organizations do not provide employees with the name and contact information of a specific point of contact when a computing device goes missing.
  - 81.5% of respondent organizations do not conduct periodic security awareness programs on computer theft.
  - 85.4% of respondent organizations do not have a written policy making employees financially responsible for computer theft if security guidelines are not followed.
  - 89.6% of respondent organizations do not have written guidelines on protecting proprietary information on computing devices while traveling.
  - 95% of respondent organizations do not have written guidelines mandating encryption of proprietary information.

A failure to employ any type of preventative solution to protect and secure computing devices and the invaluable proprietary information they contain is a formula for disaster.

### Recommendations

The best defense against computer theft is prevention. Individuals and organizations should review their security policies and implement common sense measures that include (i) the deployment of available security solutions; and (ii) the implementation of a security awareness program on computer theft. Security awareness programs should include not only how to safeguard a computer from theft, but also the ramifications of the theft and what actions to take when a computing device goes missing.

**Set clear policies and enforce them.** Organizations that take a no nonsense approach to computer theft suffer fewer losses. Make sure you have an in-place set of security guidelines that covers all aspects of your computer protection program and that employees have been properly made aware of procedures. Be prepared to enforce your policy whenever needed.

**Create awareness throughout your organization.** Computer theft threatens your entire organization. Training all employees to be aware of computer theft is perhaps the single most important investment an organization can make to prevent the loss of computing devices, proprietary information and trade secrets. Maintain awareness throughout the enterprise by posting signs and posters that reinforce the training lessons.

**Implement protective measures.** Monitor your organization's computer usage and make sure critical data is backed up on a regular basis. Be sure proprietary data files are encrypted. Use multi-layered security. For example, locks and cables will not adequately solve the problem: locks and cables can be cut; metal lockdown enclosures and whole laptop trolleys have been stolen along with their contents. In such cases, once the stolen computing device goes out the door those preventative measures are of little use. Consider using a software tracking agent in addition to these physical solutions. A tracking agent sends an invisible email message to you with the stolen computer's exact location. Police and security personnel recover the stolen property. Some tracking companies have very impressive recovery records.

**Be Proactive.** Conduct spot checks around your enterprise. If you find unattended/unsecured computing devices exposed, consider having your security personnel lift and safeguard them. Leave a highly visible form letter behind for the offender, directing them to the security office to recover their property. Perhaps a mandatory security guideline training session might be in order.

**The Bottom Line.** As bad as the statistics are, the real cost of computer theft is likely much higher. Most organizations do not realize they are a computer theft victim until weeks after the fact. Theft of a computing device that contains trade secrets can cost a large company hundreds of millions of dollars, or a startup company its only product in the marketplace. Protecting your company from computer theft doesn't have to be costly, but losses for an unprotected organization can be incalculable.

---

## About BSI

### **Brigadoon Software** inc

Brigadoon Software, Inc. is a closely held New York corporation specializing in the development and distribution of innovative computer security software products. Formed in 2000, Brigadoon

Software has grown into the largest provider of computer tracking and theft recovery software in the world to both the Windows and Macintosh communities. Brigadoon Software's Award Winning Flagship software products, PC PhoneHome™ and MacPhoneHome™ have been internationally recognized as "Best of Brand."

For more information, contact:

Brigadoon Software, Inc.  
143 Main Street  
Nanuet, New York 10954  
Tel: +1-845-624-00909  
Fax: +1-845-624-0990  
Website: [www.brigadoonsoftware.com](http://www.brigadoonsoftware.com)  
Email: [sales@brigadoonsoftware.com](mailto:sales@brigadoonsoftware.com)

## Reprint Guidelines

Permission to reprint and/or distribute 2003 BSI Computer Theft Survey results:

Brigadoon Software, Inc. grants permission to distribute and reprint the 2003 BSI Computer Theft Survey logo and survey results as long you republish according to the following criteria:

1. The 2003 BSI Computer Theft Survey results are not altered in any way.
2. The Brigadoon Software Inc. contact and copyright information are not removed from the survey results.
3. If excerpts of the graphics of the 2003 BSI Computer Theft Survey are used in print, the following attribution must be included within the graphical box: "Source: 2003 BSI Computer Theft Survey ([www.brigadoonsoftware.com](http://www.brigadoonsoftware.com))."
4. If excerpts of the text of the 2003 BSI Computer Theft Survey are used in print, the following attribution must be included within the paragraph in which the excerpt is used: "according to the 2003 BSI Computer Theft Survey ([www.brigadonsoftware.com](http://www.brigadonsoftware.com))."
5. If excerpts of either the text or graphics of the 2003 BSI Computer Theft Survey are used online, in addition to complying with the attribution guidelines for text and graphics above, a hyper-link must be added to the "[www.brigadoonsoftware.com](http://www.brigadoonsoftware.com)" attribution.