



# Symantec 2005 Pulse of IT Security in Canada

Volume III

# Pulse of IT Security in Canada

## Contents

<b>Key findings</b> .....	4
Importance of IT security .....	4
Risk of attack .....	4
Disclosure of security breaches .....	4
Virus/worm infections .....	5
Approach to IT security .....	5
Investment in IT security .....	5
<b>Introduction</b> .....	6
<b>IT security as a top priority</b> .....	6
<b>Risk of attack</b> .....	8
<b>Nature of the threats</b> .....	10
<b>Preparation, prevention, and management</b> .....	11
<b>Current investments and prevention measures</b> .....	12
<b>Resolving a security breach</b> .....	14
Viruses .....	15
<b>IT security spending trends</b> .....	16
<b>Conclusions</b> .....	18

With attacks on IT infrastructures on the rise and continued discovery of vulnerabilities and exploits, attention continues to be focused on more effective ways of preventing and managing breaches in IT security.

The annual Symantec Pulse of IT Security in Canada survey, now in its third year, assesses how key decision makers view and respond to IT security challenges in Canadian enterprises. This report highlights changes over the past 12 months.

### **Key findings**

#### **Importance of IT security**

- IT security is rapidly making its way up the list of key enterprise priorities, with 77% now rating security as a top-5 priority, up 18.5% over last year.
- Concern continues to grow with 41% more concerned about IT security than they were 12 months ago, although marginal growth in concern may be slowing somewhat.
- The Top IT security driver is protection of data and information. Compliance with legislation and regulations emerged strongly this year as a second main factor.

#### **Risk of attack**

- Overall, enterprises consider their risk of attack to be moderately-low and their capability to protect themselves as moderately-high.
- Primary security attacks experienced were viruses/worms (76%), spam (65%), and spyware (62%).
- Enterprises are concerned with a broader range of security threats this year, in contrast to predominant concern last year for viruses/worms. Primary threats of concern are: external unauthorized access, viruses, and unauthorized access by insiders.

#### **Disclosure of security breaches**

- Only 38% of respondents would admit to a security breach.
- 97% of those that would admit to a breach have been a target, up from 80% in 2004 and 19% in 2003.

### **Virus/worm infections**

- Viruses/worms are a less predominant issue on the minds of IT executives compared to 2004.
- Top perceived threats: data & information protection and lost employee productivity.
- Frequency of infection is shifting to yearly from quarterly. Nevertheless, many enterprises are still inadequately protected.

### **Approach to IT security**

- Most claim to be proactive, however many have no security policy in place, no procedures to manage vulnerabilities and patches, no formal incident response plan, and no incident response teams.
- Emphasis is shifting to security delivery by IT security specialists from IT generalists. Also, there has been substantial growth in the use of external security partners.

### **Investment in IT security**

- A median of 6% of total IT budget is allocated to IT security.
- Budgetary optimism is high, with half anticipating increases in security budgets.
- Areas of planned investment include a broader range of proactive measures than in previous years, including security policies, real time monitoring, and more focus on security training.

**Introduction**

This third annual Symantec Pulse of IT Security survey in Canada was conducted in April and May 2005 to assess the viewpoints of Canadian IT executives regarding IT security. One hundred senior executives with security responsibility from Canadian enterprises with revenues of greater than \$50 million were interviewed on topics such as the importance and costs of IT security in their organizations, their perceived risk of a security breach, and current and future measures they are taking to protect their organizations from security attacks and breaches. This report summarizes the key findings from this survey.

**IT security as a top priority**

IT security continues to make its way towards the top of corporate priorities in enterprise-level Canadian organizations. The trend towards increasing emphasis on IT security continues, with IT security cited more and more as a top-5 corporate priority. Moving into 2005, 77% now rate IT security as a top 5 corporate priority for their organization. With YOY (year-over-year) increases of 18.5% in 2005 and 6.6% in 2004, IT security is rapidly making its way into the list of key priorities facing enterprise-level organizations in Canada.

Heightened level of concern about IT security remains a prominent feature, with nearly all reporting that their level of concern is as high (56%) or higher (42%) this year than it was last year. Although continuing to rise, marginal growth in rates of concern has levelled off somewhat this year with 23.6% YOY fewer reporting that they were more concerned this year than did so in the 2004 survey (Figure 1).

**SURVEY SPECS**

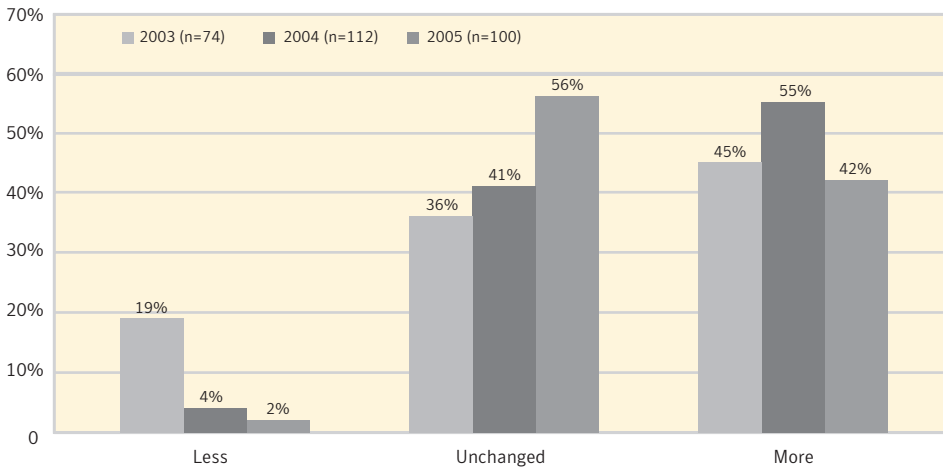
**Target**  
Canadian enterprises, revenues > \$50 million

**Respondents**  
Senior IT Executives with responsibility for enterprise security

**Respondent Type**  
VP IT/IS, CIO, Officer / Director / Architect of IT Security, etc.

**Timeframe**  
April–May 2005

**Total Respondents**  
100

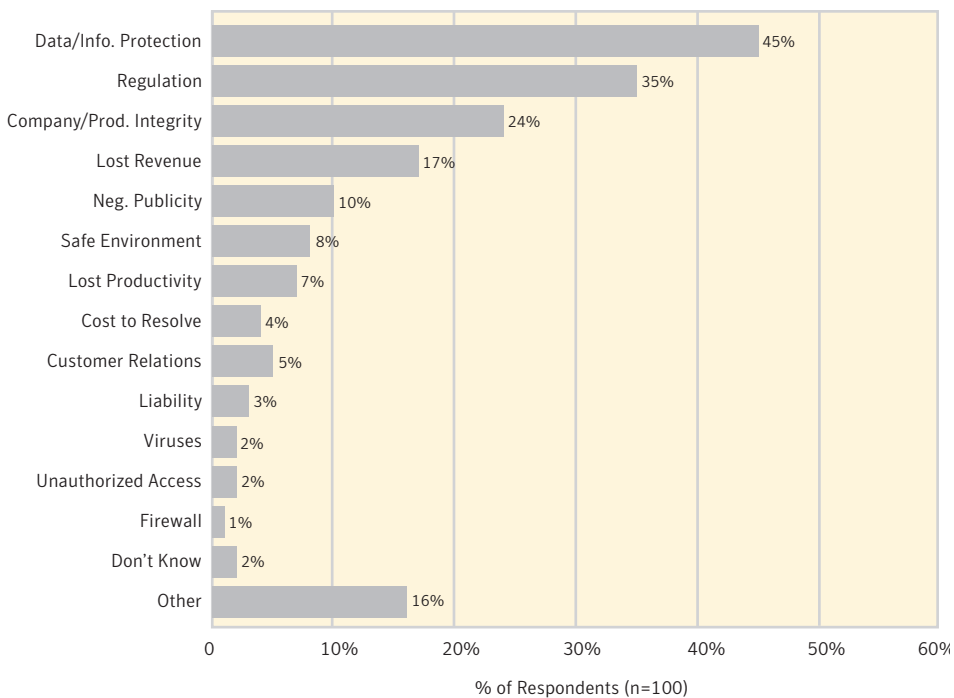


**Figure 1: Level of concern about IT security compared to 12 months ago**

## Pulse of IT Security in Canada

Nevertheless, IT security is a “hot” issue of increasing importance and relevance to these organizations as evidenced by over 51% expressing willingness to participate in a follow up focus group study on this topic. This willingness to participate is up 46% YOY from last year, suggesting growing interest, relevance and perhaps urgency of the IT security issues and challenges facing these executives. This response is high compared to recent similar non-security related IT studies, where respondents’ willingness to participate in follow-up focus groups was typically close to nil.

Protecting data and information assets continues to be the leading driver for attention to IT security, cited as a top 3 priority by 48%, similar to the 45% last year. Compliance with legislation and regulations has emerged as the second main driver (35%) up 119% year-over-year, displacing the secondary concerns from last year about lost revenue due to business disruptions.



**Figure 2: Top 3 drivers of IT security**

When asked about what was the most important driver of enhanced attention to regulatory compliance, the leading responses were customer requirements (27%), Canadian Government (24%) and US Government (13%). When asked about second most important drivers, Canadian Government predominated being cited by an additional 30% of respondents. Rapid growth of compliance issues likely reflects the impact on these enterprises of recent Canadian and USA legislation for personal information and privacy protection, and in particular, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into force in Canada in 2004.

### Risk of attack

Canada's IT executives are cautiously optimistic about the risk they face and the measures that they have in place to counter potential breaches. Despite heightened concern about IT security, they express moderately-high confidence (median 8 out of 10) in the capability of their organization to protect itself from attacks and prevent breaches (Figure 3). Nevertheless, this also indicates some level of doubt about their ability to ensure that the enterprise is protected.

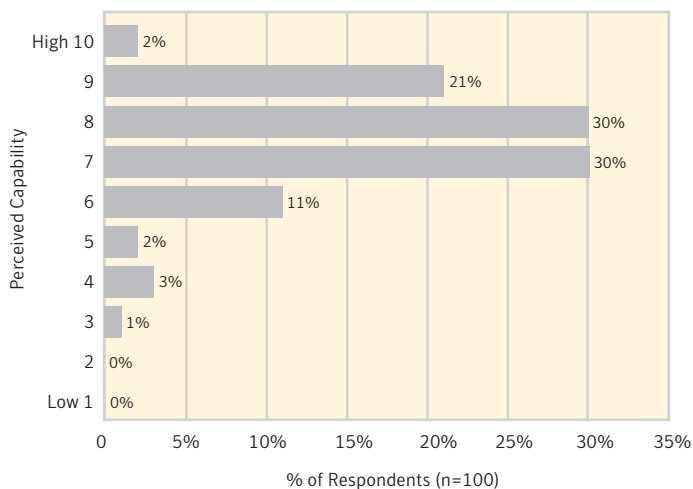
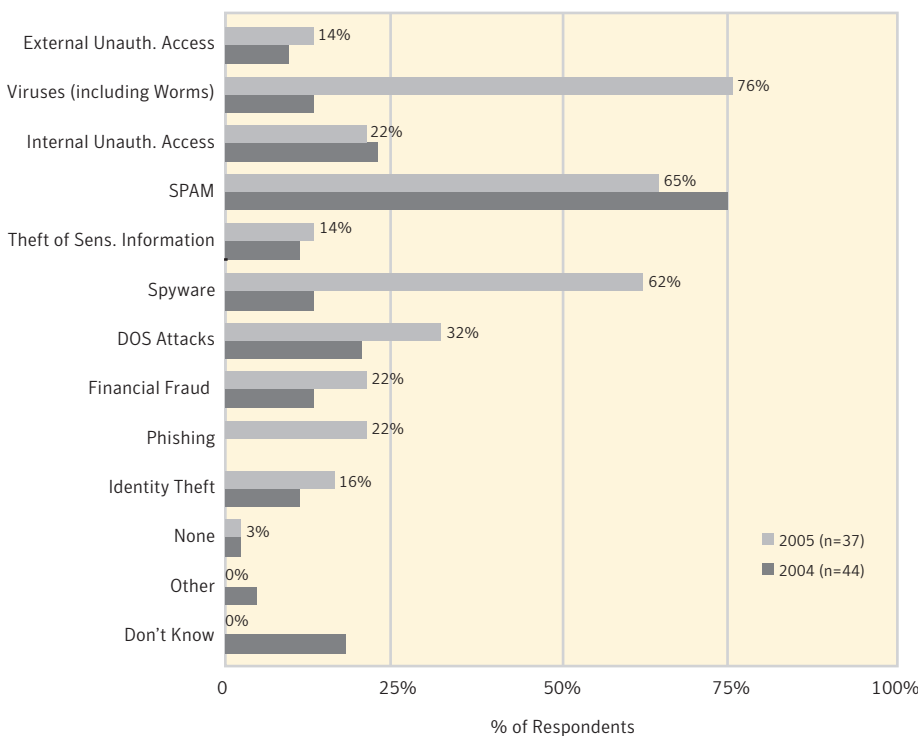


Figure 3: Perceived capability of organization to protect itself from security attacks and breaches

Similarly, they feel relatively secure about their organization's risk of being negatively affected by a security attack or breach. When asked to rate their risk of being attacked on a scale of 1 (low) to 10 (high), as a group, their response is characterized as a perception of "moderately-low" risk, with a modal value of 3 out of 10 and over half rating their risk at 4 out

of 10 or less. This characterization (and distribution of individual responses) has not changed significantly from either 2004 or 2003.

The incidence of attacks on IT infrastructure is on the rise and this problem is pervasive—likely all have been affected to some extent during the past year. Although only 38% of organizations would admit (even privately) to a security attack or breach, 97% of these reported that they had actually suffered from an attack or breach during the past year, up from 80% in 2004 and only 19% in 2003. The majority had suffered from viruses (76%), spam (65%), and spyware (62%) attacks (Figure 4).



**Figure 4: Security breaches experienced**

This year has seen substantial changes in the threat-landscape. Reports of virus attacks grew five-fold and spyware emerged as a rapidly growing threat category with over four-fold growth year-over-year. Similarly, phishing was added as a new threat category to this survey and was reported by nearly a quarter of the respondents who would admit to any attacks or breaches.

### Nature of the threats

IT security threats take a range of forms, including viruses and blended threats, external unauthorized access (hackers and crackers), unauthorized activities by insiders (either intentional/disgruntled or unintentional/accidental), identity theft (fraud/customer information), denial of service attacks, spam, and many others. Although all continue as threats for Canadian organizations in 2005, there has been a shift in year-over-year concern for each.

In 2005, no single IT security threat predominates as being the most important concern of IT executives, in contrast to 2004 when virus attacks were the dominant concern rated as being most important (Figure 5 panel 1). This year, a broad range of threats are cited more equally (and at lower frequency) as being most important, including external unauthorized access, viruses, internal unauthorized access and a wide variety of other categories (Figure 5). Although viruses remain as a substantial concern, last year's focused apprehension has passed which suggests that respondents have a reasonable degree of confidence in the capability of existing measures to handle these threats.

Considering the three most important concerns combined (Figure 5 panel 4), in 2005 the leading concerns are external unauthorized access (58%), followed by viruses (49%) and

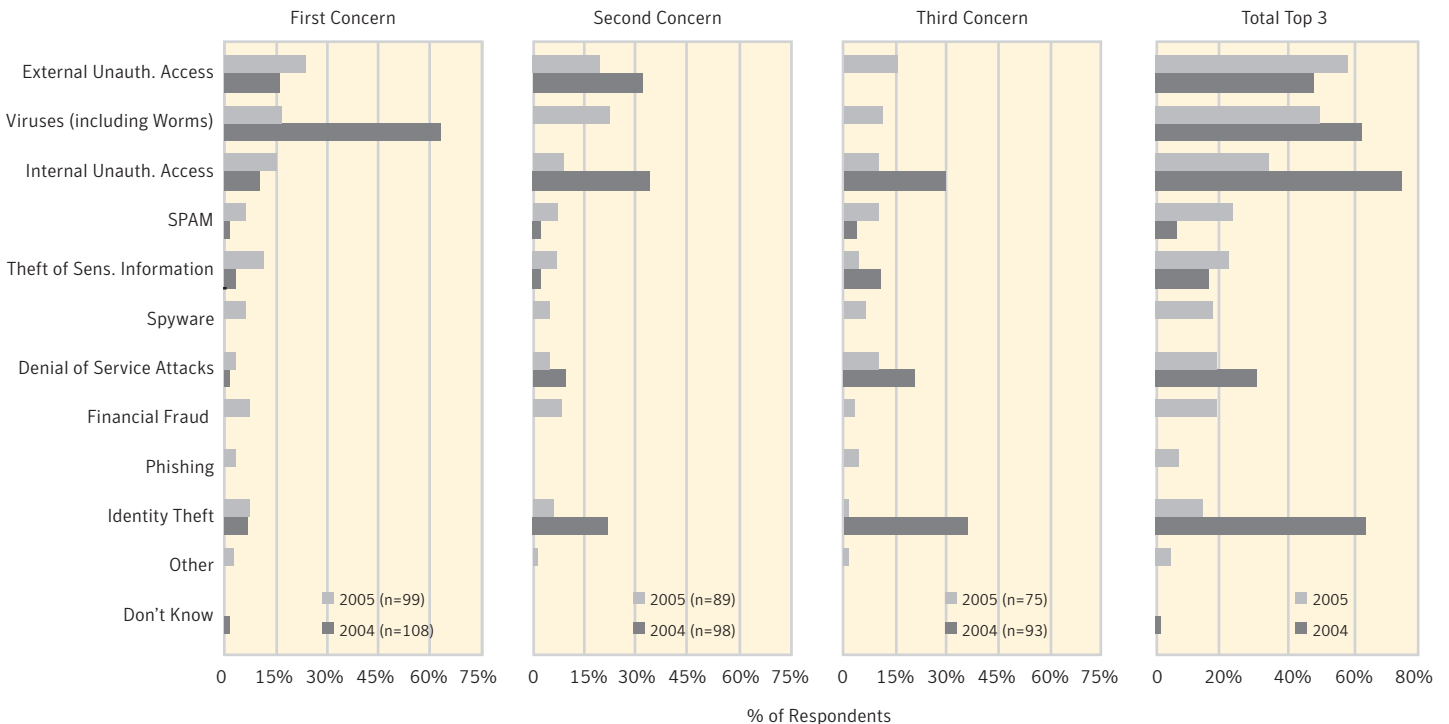


Figure 5: Ranking of IT security threats

unauthorized access by insiders (34%). Compared to 2004, concern has shifted from threats posed by insiders to attacks and breaches perpetrated by outsiders.

Overall, viruses declined 22% as a top 3 concern compared to 2004, despite the continued pervasive nature of these threats (see Figure 5, page 10).

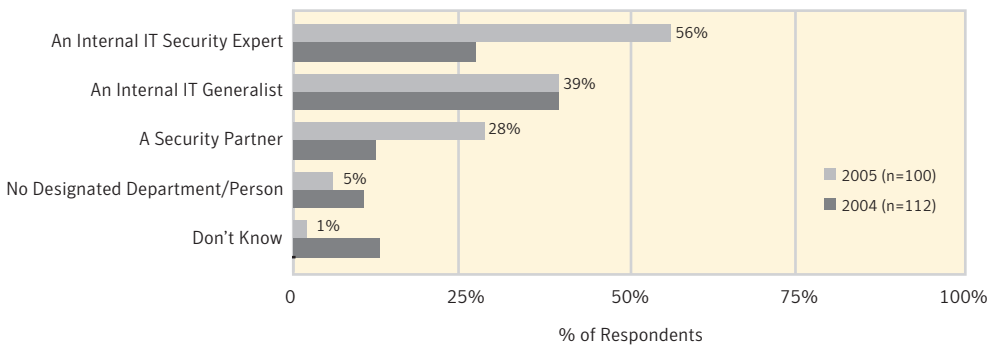
Spam is a growing concern for these enterprises with a nearly four-fold increase in ranking as a total top 3 concern. Spyware emerged as a strong threat concern in 2005; mirroring the growing incidence of spyware attacks reported previously in this survey report (see Figure 4, page 9).

Conversely, unauthorized access by insiders and identity theft declined dramatically as total top 3 concerns, compared to 2004 when they were strongly represented as threats of secondary and tertiary priority.

**Preparation, prevention, and management**

Most (84%) organizations claim that they take a proactive approach to security. Nevertheless, many admit that they primarily respond to crises, do not have a corporate IT security policy in place (24%) to guide their actions, have no formal procedures in place to manage vulnerabilities and implement patches (25%) and have no formal incident response plan in place (40%) that would be initiated immediately should a security breach occur. Although the majority claims to be proactive, there is still room to improve the overall level of IT security preparation, prevention, and management.

A major shift is underway in how security is addressed. Organizations are investing in security specialists, both in-house and out-sourced (Figure 6). In 2005, 56% now use internal IT security specialists to prepare for and deliver their IT security programs, more than double the previous year.



**Figure 6: Responsibility for IT security planning and delivery**

There has been similarly dramatic growth in outsourcing as many organizations move towards external security specialist partners to supplement their internal general IT capability. This shift towards specialization is not complete, with most organizations using a mixture of internal security specialist, internal IT generalists, and in many cases external security partners.

Of those using external security partners, the majority (64%) rely on an external partner for up to 33% of their security needs with an average of 18% handled by the external security partner. A smaller group (18%) outsources most of their security needs with an average of 86% handled by security partners. Overall, a single security partner is the norm, however 39% rely on multiple partners. Satisfaction with external security partners is high with a modal rating of 8 out of 10. Only 14% rate their satisfaction as moderate (five) or lower.

### Current investments and prevention measures

Last year, the top 4 areas of planned investment included antispam, antivirus, security training, and firewalls. To date, most organizations are well on their way to addressing the tactical issues of antivirus protection (89%), firewalls (85%), and antispam measures (67%) (Figure 7). However, only a small proportion has yet to deploy anti-spyware measures, despite the dramatic increase in spyware breaches reported by these organizations (see Figure 4, page 9).

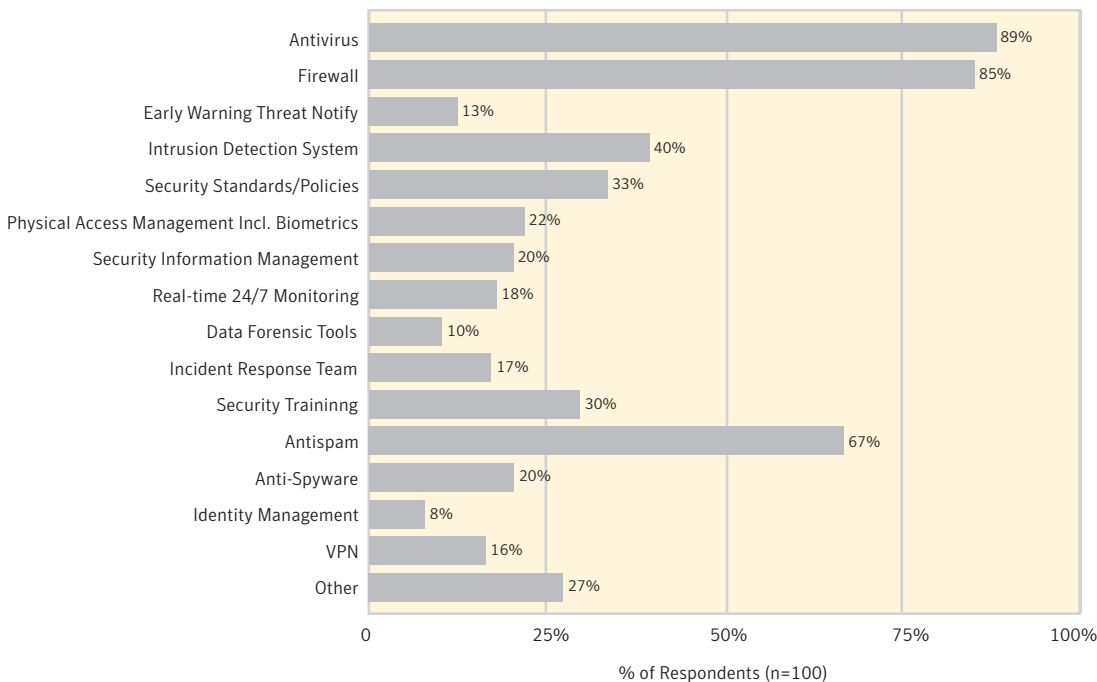


Figure 7: IT security measures deployed to date

Many of the fundamental security tools are now in place. However, there is still much more that these enterprises can do to move beyond crisis response to engineer-in processes and procedures to make themselves less vulnerable. To this end, a variety of other more strategic and potentially proactive measures have been initiated by some organizations but have yet to be implemented on a widespread basis. Examples of these measures include active intrusion monitoring, early warning security threat notifications, real time information security monitoring, development of critical incident response plans and teams, among others. Current status of many of these measures is summarized below.

- **Active intrusion monitoring**—Approximately 10% admit that they do not monitor their networks for intrusion at all. Although most claim to monitor their networks for intrusions, the degree of coverage varies widely. Less than half (43%) have implemented active intrusion monitoring with substantially complete network coverage (e.g. >90%), compared to 54% in 2004.
- **Monitoring & review firewall logs for inappropriate activity**—Because firewalls are gateways between networks of varying trust levels, the frequency at which logs are monitored is critical to timely detection and creating alerts as quickly as possible. Despite the importance as a physical first line of defense, fully 18% only review logs monthly or less frequently (including those who only review logs after an incident has occurred). Daily review is the standard of practice in just over half and a further one-quarter monitor logs weekly. This situation has not changed significantly since last year's survey.
- **Monitoring of critical application servers for unauthorized access or use**—Approximately one-fifth of respondents admit that they are not monitoring their critical application servers for unauthorized access or use, up from 10% in 2004.
- **Vulnerability scans of networks and critical services**—Most organizations report that they conduct vulnerability assessments. Vulnerability assessments are most commonly conducted on a quarterly (25%), yearly (22%), and monthly (17%) basis, representing a slight shift towards more frequent assessments compared to last year. Still, eight percent admit to addressing this either only after a critical incident or not at all.
- **Perimeter penetration testing**—Yearly testing is the norm by over half of organizations in this survey. Only 28% conduct perimeter penetration testing on a quarterly or more frequent basis and a further 12% either don't know, never do it, or only test reactively after a critical

penetration incident. This pattern is generally consistent with that in 2004, although many more respondents did not know last year.

- **Formal procedures to manage vulnerabilities & implement patches**—Time to patch is short, with an average 5.8 days between announcement of a vulnerability and emergence of exploits and an average of 48 new vulnerabilities announced each week. Despite this risk, approximately one-quarter of respondents admit that they still have no formal procedures in place to manage the proliferation of vulnerabilities and implement patches, slightly improved from last year when one-fifth lacked this capability.
- **Incident response plans:** 60% claim to have developed an incident response plan that could be implemented immediately should a security breach occur, compared to 69% in 2004.

### **Resolving a security breach**

The total costs of addressing attacks and resolving a security breach can extend far beyond the costs of the technology and time of IT personnel required to resolve the problem. Additional costs include those directly or indirectly attributable to disruption of business operations, loss of data and information, reduced network level of service, lost employee productivity, exposure to liability, impact of negative publicity, and a wide variety of others. Typically, many of these costs are often poorly quantified and poorly tracked by traditional accounting or business performance metrics. As such, full cost impacts of security breaches are likely underestimated.

Many enterprises are reticent to discuss their negative experiences and costs incurred as a result of security breaches. For those willing to discuss the impacts of security breaches during the past year, many confirmed that costs were poorly tracked and 20% could not estimate them at all. An additional 20% indicated that they had no costs during the past 12 months (although most of these had admitted to suffering from a security breach during this period), further suggesting inadequate cost tracking or additional reticence to disclose these data. Of those who provided cost information, estimates ranged from less than \$5K by approximately one-quarter of respondents, to between \$10K and \$500K by the remainder (Figure 8, next page).

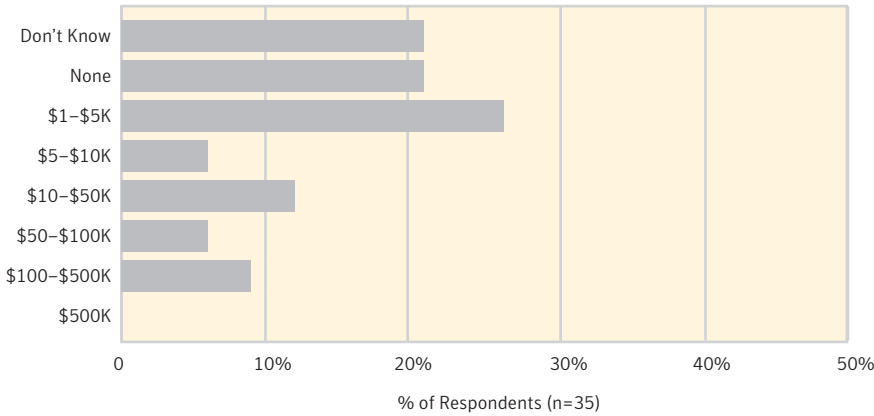


Figure 8: Estimated total cost of IT security breaches

The primary costs of security breaches to these enterprises (Figure 9) consist of lost employee productivity (39%), IT personnel costs (32%), followed by technology expense (18%). Notably, the costs of technology are minimal compared to the combined people and productivity costs to the organization.

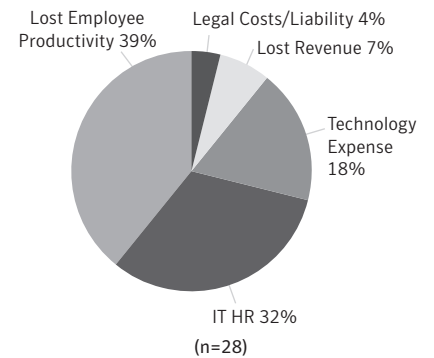


Figure 9: Primary costs of security breaches

**Viruses**

Viruses (including worms) continue as a concern in 2005 but are not the predominant issue on the minds of IT executives that they were last year. Overall, progress has been made with modal frequency of infection shifting to yearly (32%) from quarterly last year (Figure 9). Nevertheless, many organizations are inadequately protected and this is a more frequent problem for them with 29% reporting that they experience virus infections on a monthly or more frequent basis. As with last year, a surprising proportion of the organizations surveyed claimed to experience virus infections on a daily basis.

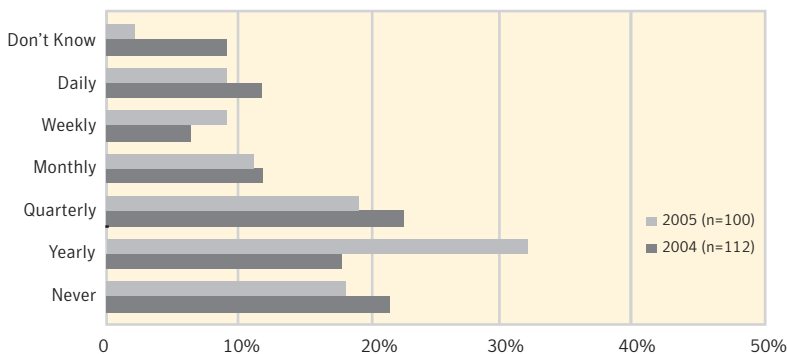


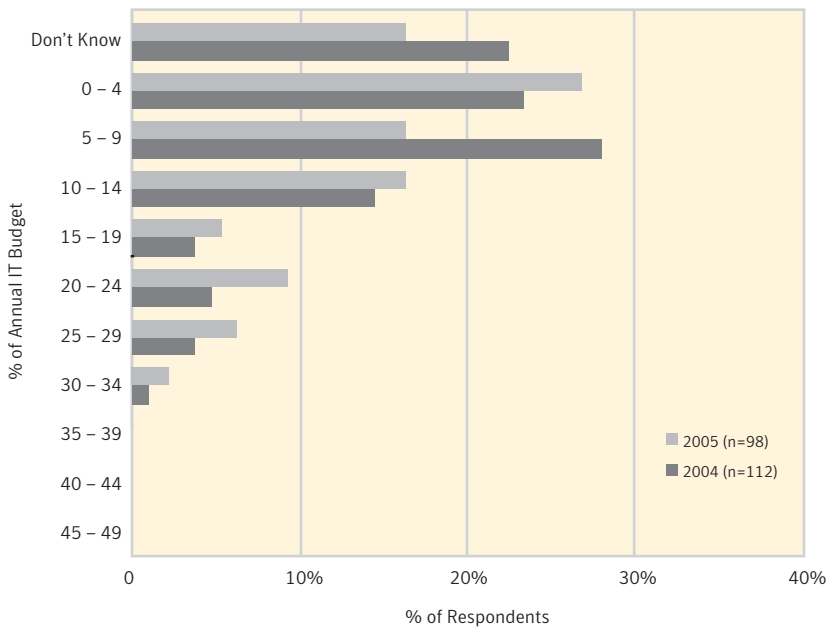
Figure 10: Frequency of virus infections

The most serious threats from virus outbreaks are considered to be data and information protection (30%) and lost employee productivity (29%) as highest priority concerns. Similar to last year, the lowest ranked concerns included: negative publicity, legal or liability ramifications, and the cost of resolving the outbreak.

The total costs of resolving virus outbreaks varies widely from less than \$5,000 (25%) to greater than \$500,000 (2%), with 42% reporting costs less than \$10,000 per outbreak. Nearly one-quarter of the IT executives did not have any metrics available on the cost impact of virus outbreaks to their organizations.

**IT security spending trends**

Despite the proliferation of threats and increased concern about security issues, IT security remains a relatively small portion of the overall IT budgets with median allocations of 6% in 2005 and 5% in 2004 (Figure 11). Over three quarters (77%) allocate less than 15% of their total IT budget to IT security. The remaining quarter of these enterprises allocate substantially more to security, in the range of 15–35% of total IT budgets and this smaller group of higher spenders appears to have grown compared to 2004.

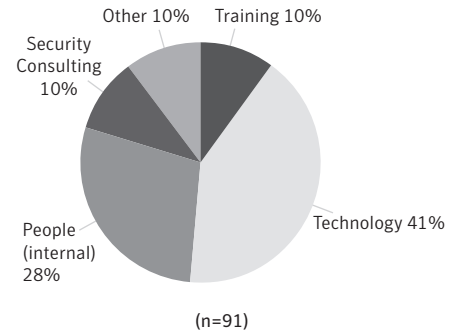


**Figure 11: IT budget allocation to IT security products and services**

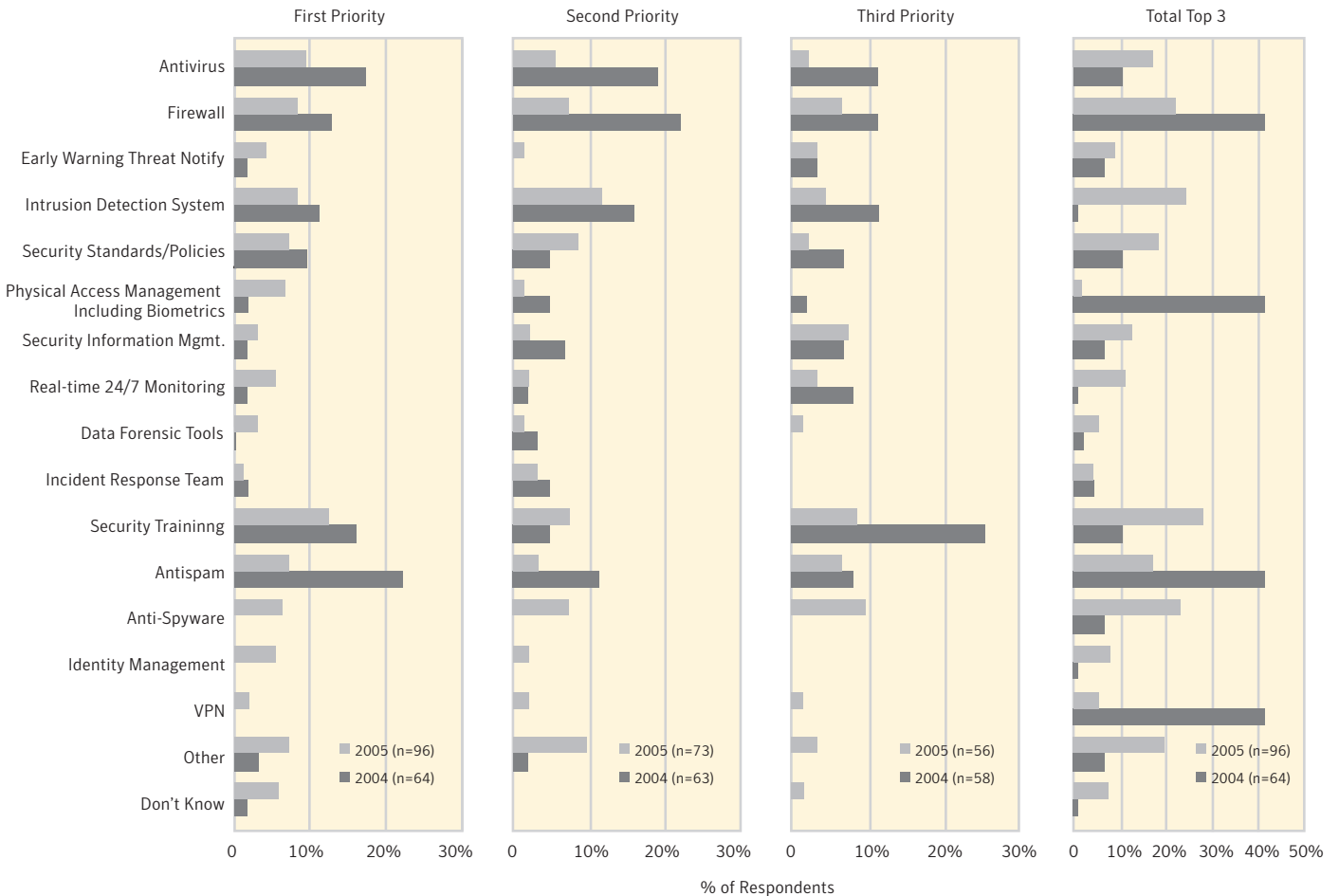
# Pulse of IT Security in Canada

In nearly all cases, security budgets have either remained stable (53%) or increased (45%) over the past 12 months, similar to the situation in 2004. Budgetary outlook is generally optimistic towards security over the next 12 months. Allocation to spending on security products and services is expected to be at least as high as currently, with increases anticipated in the next 12 months by half of the respondents.

Technology spending accounts for the largest component (41%) of IT security budgets, followed by the costs of internal security-related personnel (Figure 12). Although current spending is largely internally-focused, only 10% is invested in security training (either on security professionals or end users). Currently, spending on external security partners is similar to the investment in internal training and may well rise if the trend continues towards increasing use of external security providers.



**Figure 12: Current IT security spending breakdown**



**Figure 13: IT security investment plans for 2004 and 2005**

Respondents intend to invest in a broader range of security measures over the next 12 months than in the previous year (Figure 13). No single measure predominates security investment plans moving forward this year. This situation mirrors the pattern of concerns (see Figure 5, on page 10) in which no single IT security threat predominates in 2005 as being the most important concern of IT executives.

Last year, investment plans were strongly focused on specific tactical protection measures including antivirus, antispam, and firewalls. Investment in these measures will continue and be supplemented with investment in antispware measures by many to round out baseline defenses against blended threats. Most organizations have confidence in these measures and consider them now as ongoing base-level investments.

Security planning is now entering a second phase as organizations move beyond tactical responses to specific attacks and begin to focus on more strategic investments in a broader range of proactive initiatives, such as development of security standards and policies, intrusion detection systems, real time monitoring, and more focus on security training.

Future investment in security training is emerging strongly as a priority. Although this is expected given the observed shift towards increasing specialization of personnel who deliver security services, this has yet to show up as an increased focus on training in current IT budget allocations (see Figure 12, on page 17).

### **Conclusions**

IT security is rapidly moving to the forefront of enterprise priorities and is now front of mind for the majority of IT executives. Concern about IT security continues to increase as in previous years, although year-over-year growth in concern may be levelling off somewhat.

Protecting corporate data and information assets continues to be the leading driver of this elevated attention to IT security issues. In addition, this year saw the strong emergence of legislative/regulatory compliance as a driving force behind security activities, likely as a result of PIPEDA coming online this past year.

Enterprises are concerned with a broader range of security threats this year, in contrast to predominant concern last year for viruses/worms. Primary threats of concern are: external unauthorized access, viruses, and unauthorized access by insiders.

## Exploring Spyware and Adware Risk Assessment

Risks to the enterprise are perceived to be moderately-low and capability to protect moderately high. This outlook is best described as “cautious optimism” that leaves some doubt about future vulnerability. Most claim to have a proactive approach to IT security, however much more can be done to improve the overall level of preparedness, prevention, and ongoing management of risk exposure, particularly in the areas of active intrusion monitoring, early warning security threat notifications, management of vulnerabilities & patches, real time information security monitoring, and development of critical incident response plans and teams.

A major shift is underway in how security is addressed. Organizations are investing in security specialists, both in-house and out-sourced. Most organizations now have dedicated IT security specialists—a major change from last year. A growing number of enterprises are turning to external security partners and are satisfied with those partners. Currently, most supplement internal capability with external partner expertise; however a small proportion relies on external security partners for most of their needs. Growth in the use of external security specialist partners is expected to continue as a key trend in the future.

Despite the proliferation of threats and increased concern about security issues, IT security remains a relatively small portion of the overall IT budget with median allocations of 6% in 2005. A minority of enterprises devote a higher proportion of their total IT Budget to IT security, typically in the range of 15–35%. This group of “higher spenders” appears to be growing. The outlook is generally positive for security budgets, with increases expected in about half of these enterprises and stable budgets in the remainder.

Last year, investment plans were strongly focused on specific tactical protection measures including antivirus, antispam, and firewalls. Investment in these measures will continue and be supplemented with investment in antispymware measures by many to round out baseline defenses against blended threats. Most organizations have confidence in these measures and consider them now as ongoing base-level investments.

Security planning is now entering a second phase as organizations move beyond tactical responses to specific attacks and begin to focus on more strategic investments in a broader range of proactive initiatives, such as development of security standards and policies, intrusion detection systems, real time monitoring, and more focus on security training.

## **About Symantec**

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, California, Symantec has operations in 35 countries.

More information is available at [www.symantec.ca](http://www.symantec.ca).

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers, please visit our Web site. For product information in Canada, call toll-free 1 800 607 8661.

## **About Branham Group Inc.**

Based in Ottawa, Ontario, Branham Group Inc. is a leading "Go-to-Market" consulting firm servicing the global information technology marketplace.

Branham conducts work in the United States, Europe, Latin America, Asia and Canada.

Branham Group assists information technology companies and related institutions in achieving market success through its planning, marketing and partnering services. Branham has a strong legacy of researching and analyzing vertical, horizontal and cross-industry opportunities.

In Canada, it is well known for publishing the most comprehensive listing of the top Canadian ICT vendors ([www.branham300.com](http://www.branham300.com)).

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brand and product names are trademarks of their respective holder(s). Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Branham Group, Branham300, and the Branham Group logo are the properties of Branham Group Inc. Copyright © 2005 Symantec Corporation. All rights reserved. 06/05 10424064