



Pulse of IT Security in Canada

Volume VII



45 O'Connor Street, Suite 1150 • Ottawa, ON • Canada • K1P 1A4
Tel: 613.745.2282 • Fax: 613.745.4990 • www.branhamgroup.com

Pulse of IT Security in Canada

The annual Symantec Pulse of IT Security in Canada survey, now in its seventh 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 and provides trending data for the survey period between 2003 and 2009.

Key Findings

Importance of IT Security

- » While all respondents articulate that IT security is important, only 56% (vs. 70% last year and 82% in 2007) see it as a top 5 priority.
- » The proportion of IT security managers more concerned with IT security compared to 12 months ago fell to 24% (vs. 41% in 2008). 6% are less concerned, similarly to last year.
- » Data protection and lost revenue due to disruption of business operations were the top two concerns among respondents this year. Reputational risks declined in importance this year, with 37% of respondents ranking it among the top 3 (down from 53% last year).
- » Fewer companies have the positions of Chief Privacy Officer and Chief Security Officer (down 15% and 6%, respectively).

Coping with a Diverse Threatscape

- » The top four reported security attacks include Viruses/Worms (85%), SPAM (82%), Spyware (69%) and Security Policy Violations (67%).
- » The highest rate of growth this year occurred in Instant Messaging (up to 25% this year from 13% in 2008).
- » A new category, web application security, was reported by 20% of respondents.
- » The perceived risk of attack decreased slightly from last year, while organizations' estimate of their ability to protect themselves from an attack grew slightly.
- » 63% of respondents claim to be willing to admit a security breach publicly, down from 67% last year.
- » The annual cost of managing security breaches is driven by technology expense, human resources, lost revenue, and lost employee productivity. However, it is not believed that the full magnitude of these costs are truly understood or quantified.

Virus/Worm Infections

- » Viruses were the #1 concern of IT managers (up from #2 last year). They experienced the greatest growth

as a source of concern, with 34% more respondents listing them among their Top 3 IT security concerns.

- » The reported frequency of virus outbreaks may have fallen: the percentage reporting daily occurrences dropped slightly from 28% to 9%, while the percentage reporting infections yearly or less than yearly increased by 20%.
- » 44% of respondents estimate the cost to resolve a virus outbreak at less than \$5,000, down from 53% last year.
- » IT security managers perceive lost employee productivity (72%), compromised data/information protection (56%), lost revenue (35%) and costs to resolve outbreaks (20%) as the greatest threats from virus outbreaks.

Approach to IT Security

- » 81% of organizations report having a proactive approach to security, up from 70% last year.
- » The trend toward employing IT security specialists appears to have resumed this year, with just 48% relying on generalists for IT security issues (down from 75% last year).
- » Outsourcing use declined this year: just 49% of respondents relied on contractors to deal with IT security issues, down from 72% in 2008. The average portion of activities outsourced rose from 20% to 30% this year.
- » The use of multiple partners declined this year, with 67% using multiple partners, down from 78% last year but still up significantly from 39% in 2005.

Investment in IT Security

- » The top 3 investment plans for 2009-10 include anti-virus (42%), intrusion detection (29%), and security training (29%).
- » Median spending remains static at 5% of total IT budgets. 64% of respondents indicate that they spend less than 10% of total IT spend on security.
- » Technology (41%) and internal staff (33%) represent the majority of IT security spend.

Foreward

If the word “Complacency” captured the developments in last year’s IT Security approach among Canadian companies, this year’s budgetary pressures, combined with a more proactive approach to security among Canadian IT security groups, points toward a theme of “Making Do.”

The difficult financial environment has caused IT security to drop in relative importance on the corporate priority list this year. As a result, the proportion of respondents considering IT security a Top 5 corporate priority fell to 56% from 70% last year. According to CIO Insight magazine, security is CIOs’ ninth priority for 2010 - while important, it is clearly superseded by other concerns, such as their #1 concern of business productivity and cost reduction.¹

For the second year in a row, respondents reported that their spending on IT security decreased in the past year, with many companies planning fewer investments than usual for next year. At the same time, 81% of this year’s respondents indicated that their approach to security was proactive, up from 70% last year. Respectively, the number of reported breaches declined, in spite of a very hostile threatscape with an abundance of professional criminals launching financially motivated attacks on organizations and the information they hold on a daily basis.

IT professionals once again faced more threats than ever this year. The 2008 Symantec Internet Security Threat Report revealed several disturbing global trends:

- » There was a 19% increase in documented vulnerabilities
- » 80% of documented vulnerabilities were classified as easily exploitable, up from 74% in 2007
- » 63% of vulnerabilities affected web applications, up from 59% in 2007
- » Symantec detected 66% more phishing website hosts in 2008 than in 2007

While this has been a difficult year for both large organizations and their IT departments, complete with pressured budgets and increasing threats from outside, Canadian IT managers have managed these threats effectively thus far. The IT security toolkit of many organizations has grown quite sophisticated and mature over the past decade, but the rate of adoption for some important tools has stalled, and further progress needs to be made to deal effectively with both existing threats and new threats that are likely to arise in the future. These new threats will certainly be more sophisticated, but the proactive approach shown by Canada’s IT security managers this year should help them to continue to protect their organizations from cyber-criminals in the years to come.

¹ CIO Priorities for 2010. CIO Insight Magazine. <<http://www.cioinsight.com>>

Introduction

The seventh annual Symantec Pulse of IT Security in Canada survey was conducted in July and August 2009 to gain insight into Canadian enterprise IT security issues and trends.

One hundred senior managers with enterprise security responsibility in organizations with annual revenues of more than \$50 million were interviewed on topics such as

- » the relative importance and drivers of security;
- » perceived vulnerability to a security breach;
- » preparedness, processes and key investment areas for dealing with security breaches;
- » current approaches to security management; and
- » costs and planned spending on IT security in their organization.²

This year's respondents represent a diverse cross-section of the Canadian economy, with 35% of the respondents coming from the High-Tech, Manufacturing and Energy sectors.³

This report summarizes key findings from the survey and compares this year's responses to those from 2003-2008 where relevant. Differences by industry, while not statistically significant, are also highlighted in some instances to provide additional perspective on movements in select industry segments.

SURVEY DATA

Targets:

Canadian enterprises
Revenues > \$50 million

Respondents:

Senior IT managers and executives
responsible for enterprise security

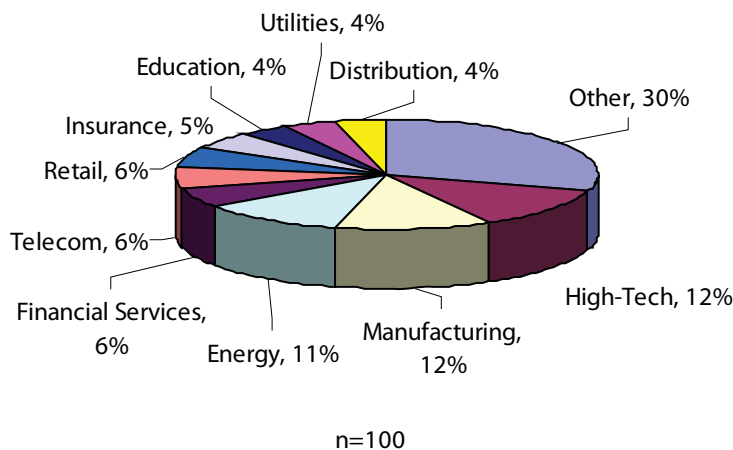
Respondent Type:

VP IT/IS, CIOs, Security Managers, Directors
of IT Security, IT Security Architects, etc.

Timeframe: July-August 2009

Total Respondents: 100

Figure 1 - Respondent Industries 2009



² The surveys conducted in 2005 - 2009 all contained the same questions, but differ from 2003 and 2004 in some elements, precluding comparison on these elements. In addition, some answer choices in multiple-choice questions were changed during the 2005-2009 period.

³ With a total sample of 100 respondents in 2009, sectoral data is not deemed statistically relevant, but may provide indicators of new or ongoing developments in those segments.

Importance of Enterprise Security

During the 2008-2009 period, the main concern for many large organizations has been difficult economic conditions, which has resulted in a relative drop in IT security as a priority. While most large organizations have made substantial investments into security, this year's conditions put pressure on IT security budgets. At the same time, however, respondents have indicated that they are increasingly taking on a proactive approach to IT security and continue to be concerned about IT security threats.

Since 2003, this study has tracked a shift of IT security from an IT domain to one that was strategic and that garnered increasing attention from senior executives. During the past two years, however, this shift has slowed as organizations focused on financial priorities.

Priority of IT Security Drops Again, Even as Concern about IT Security Rises

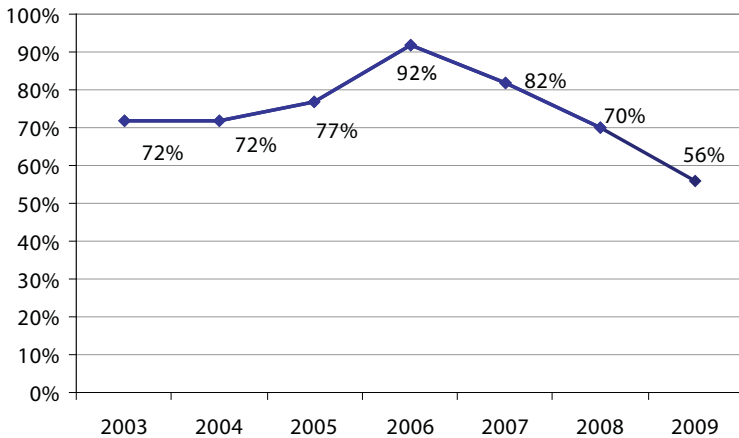
While all respondents indicated that IT security was a priority for their organizations, the proportion of respondents indicating that it was a Top 5 corporate priority this year dropped to an all-time low of 56%. This represents the continuation of a reversal in the importance of IT Security during 2007-2009, after a rise during the 2003-2006 period.

Two major reasons appear to be responsible for this decline. First, respondents were affected by the difficult financial environment, which displaced the importance of information technology management on the list of corporate priorities this year. Second, many respondents indicated that IT security was now woven into the fabric of their day-to-day operations and concerns, and was considered a priority within the IT department, even though it was not a major part of the organization's current strategic initiatives.

The drop is, however, somewhat disconcerting, considering that 24% of respondents this year were more concerned about IT security than they had been in 2008. This is in contrast to just 6% of respondents who were less concerned about IT security this year than last year. A lower ranking on the list of corporate priorities can result in difficulties finding the budgets to make important IT investments to protect organizations and their client's personal information. In fact, more respondents noted a reduced budget this year, with fewer respondents indicating increases.

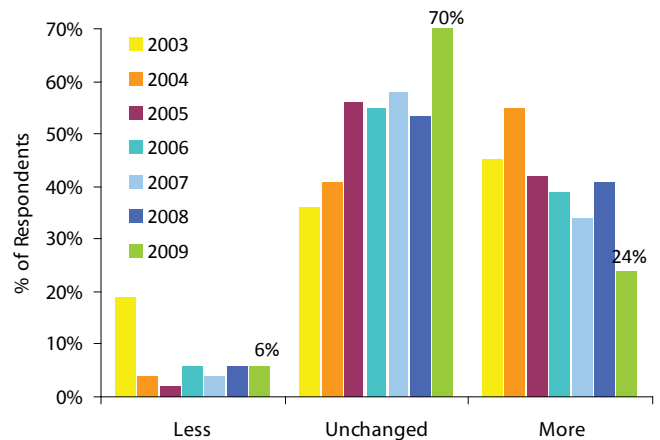
This year, there were once again interesting differences between sectors in terms of their likelihood to name IT security a Top 5 corporate priority. The Retail, Insurance, and Manufacturing sectors were the most likely to rank IT security highly on the list of corporate priorities, with the lowest results coming from the Utilities, Distribution, and Education sectors. Please note that these results are not statistically significant due to low sample sizes.⁴

Figure 2 - % Indicating Security as a Top 5 Priority (2003-2009)



n=74 (2003); n=112 (2004); n=100 (2005); n=100 (2006); n=98 (2007); n=103 (2008); n=100 (2009)

Figure 3 - Level of Concern about IT security compared to 12 months ago



⁴ n = 4-13, depending on industry

More Respondents Indicating Proactive Approach, Which Continues to Pay Off

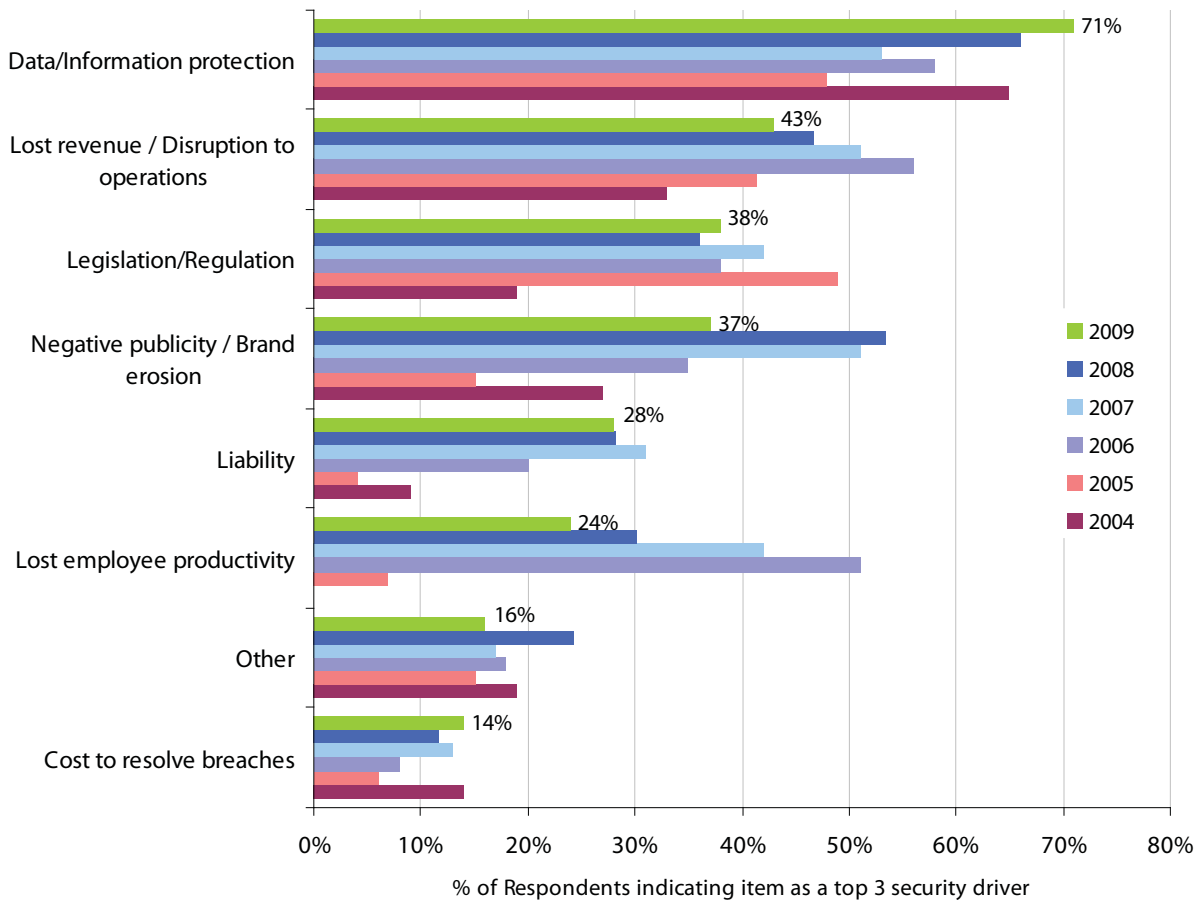
This year, 81% of respondents⁵ reported having a proactive approach to IT security, up significantly from 70% last year. In 2008, 83% of those respondents who had reported being less concerned about IT security that year had also reported a proactive approach, indicating that their efforts had been paying off. In 2009, all of the respondents who were less concerned about IT security than they had been in 2008 reported having a proactive approach to IT security in place.

Part of the rise in the proportion of respondents indicating a proactive approach could also be due to the difficult financial environment respondents faced in 2008-09. While IT security budgets have faced some pressure during this period, the threat of attack also rose, increasing the need to protect important information in a difficult time.

Attention to IT Security Driven Primarily by Protection of Information and Revenue

The top driver of companies' attention to IT security this year was once again data/information protection (ranked #1 by 39% of respondents). The second biggest concern was negative publicity (ranked #1 by 16% of respondents), followed by legislation/regulation (ranked #1 by 15%). Please see Figure 4 below for the frequency of each major security driver among the Top 3 concerns listed by respondents.

Figure 4 - Top 3 Drivers of Security (2004 - 2009)



n=112 (2004); n=100 (2005); n=100 (2006); n= 100 (2007); n=103 (2008); n=100 (2009)

⁵ n = 98

Data/Information Protection has continued to be the #1 concern of large organizations. This category includes the protection of crucial business information, as well as the protection of client data. This year, the importance of data protection as a Top 3 security driver increased 5% to 71% of respondents, which is up 23% from a low of 48% in 2005. Respondents from the Energy, Telecommunications and Distribution sectors were most likely to list data protection as their #1 concern.

Lost revenue due to disruption of business operations was the second most important IT security driver this year. While the proportion of respondents listing it among their Top 3 concerns declined by 4% this year, it is still up by 10% compared to 2004. While the relative importance of this driver is very high, the steady decline in its presence as a Top 3 priority since 2006 is likely due to the fact that many respondents feel more comfortable with their ability to mitigate the threats posed by a potential breach through a proactive approach to IT security (the percentage of respondents reporting a proactive approach increased during this time). Lost revenue was most likely to be listed as the #1 concern by Manufacturing, Distribution and Retail companies.

Legislation/Regulation was ranked among the Top 3 drivers of security by 38% of respondents this year, up from 36% last year and 19% in 2004. However, it was only ranked #1 by 8% of organizations and its presence in the top 3 is still down 11% from its all-time high of 49% in 2005. Legislation was most likely to be listed as the #1 driver by respondents from the Insurance and Utilities industries.

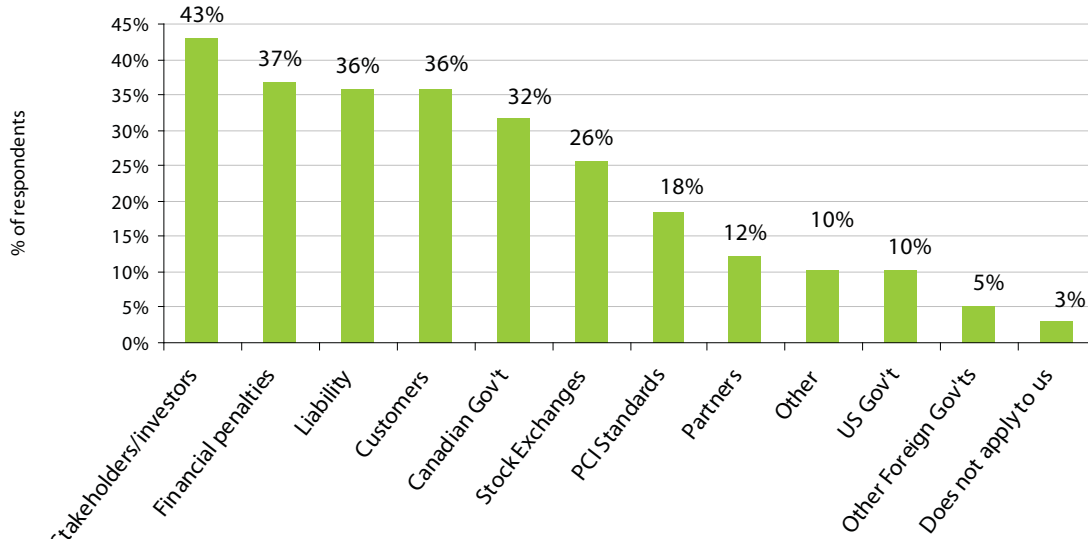
Reputational Risks including negative publicity and brand erosion declined slightly in importance this year, as 37% of respondents ranked it among the Top 3 security drivers, down from 53% last year. This is still up significantly from 27%, when the question was first asked in 2004. The decline in relative importance of reputational risks may point to a decline in highly publicized incidents of this nature in the past two years; however, it is more likely that this concern has simply been edged out by concerns about revenue and regulations during a difficult budgetary period. Once again, Financial Services and Telecommunications companies were most likely to list negative publicity as their #1 concern.

Attention to IT Legislation is Financially Driven

When asked to rank the top drivers behind their organizations' attention to IT security legislation, the drivers which were most often listed among the Top 3 were:

- » Stakeholders and investors' demands for better governance (43%)
- » Financial penalties (37%)
- » Liability (36%)
- » Customers (36%)

Figure 5 - Key Legislative/Regulatory Drivers (Frequency in Top 3)



n=98 (2009)

The drivers which were most frequently ranked #1 were:

- » Customers (16% of organizations)
- » Risk of legal actions (15%)
- » Stakeholders and investors' demands for better governance (12%)
- » Canadian government (12%)
- » Stock exchanges (12%)

This year, the top four legislative/regulatory drivers were in some way financially motivated, with Investors, Financial penalties, Liability and Customers rounding out the top four. Customers and Partners were the two categories that enjoyed the greatest growth this year: the importance of Customers grew by 7% to 36% of respondents this year, while the importance of Partners grew by 8% to 12%.

The importance of stock exchanges (a category which includes regulations such as the Sarbanes-Oxley Act) fell by 17% to 26% this year, after rising from 21% in 2005 to 42% in 2008. This decline is likely indicative of the fact that organizations subject to these regulations have largely adjusted to their requirements.

A new category was added this year based on last year's responses: PCI Compliance. This year, PCI compliance was a Top 3 legislative driver for 18% of respondents.

Finally, the number of respondents who claimed that regulations did not apply to them remained at a low 3% (up from 2% last year, but down from a high of 12% in 2007), indicating a realistic approach to regulations.

Risk of Attack

Respondents Feeling More Secure and More Prepared This Year

During the 2005-2008 period, there was a disconcerting trend toward an increase in the perceived risk of attack coupled with a decrease in perceived preparedness to deal with attacks among respondents. However, this year, the trend has reversed, with respondents indicating that they were more prepared to handle breaches (an average of 7.94 out of a maximum of ten, up from 7.48 last year). In addition, respondents indicated they felt slightly less vulnerable in terms of their probability of experiencing a significant breach, with the average perceived risk this year down from 4.9 to 4.72.

This, however, is also somewhat disconcerting, since organizations are actually more at risk this year than they were last year; for instance, Symantec found a 165% increase in new malicious code threads in 2008 over 2007.⁶ This suggests that as organizations build up their IT defenses, they are at risk of complacency about new threats to their environment and the real risk they face.

The industries which indicated the highest perceived risk this year included education, utilities, and insurance. Those with the lowest perceived risk to an IT security breach included manufacturing and high-tech. The industries with the highest perceived preparedness were high-tech, telecommunications and energy; those who felt least prepared included distribution, education and manufacturing.

Figure 6 - Risk of Security Breach vs. Preparedness

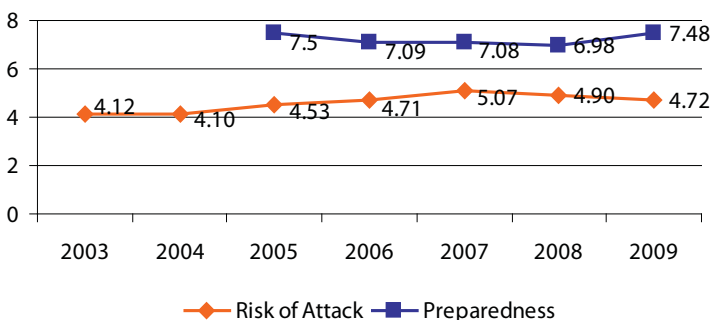


TABLE 1
RISK VS. PREPAREDNESS

Year	Perceived Risk (1=low; 10=high)	Perceived Preparedness (1=low; 10=high)
2003	4.12	n/a
2004	4.10	n/a
2005	4.53	7.50
2006	4.71	7.09
2007	5.07	7.08
2008	4.90	6.98
2009	4.72	7.48

n=73 (2003); n=108 (2004); n=100 (2005); n=99 (2006); n=98 (2007); n=89 (2008); n=99 (2009)

⁶ Symantec Internet Security Threat Report, Volume XIV. April 2009. <<http://www.symantec.com/business/theme.jsp?themeid=threatreport>>

Willingness to Disclose Breaches Declines Slightly

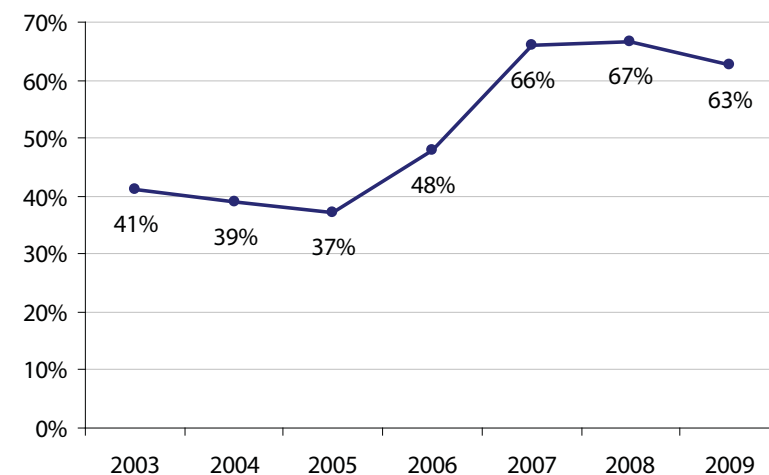
After stagnating during the 2007-2008 period, the proportion of respondents willing to disclose breaches in 2009 actually declined slightly to 63%. While this is still an improvement from the early years of the study, it appears that many companies are not willing to do more than what is legally required to disclose breaches, likely because of the potential impact on reputation and revenue that could result. Notably, Canadian companies are not compelled by law to disclose security breaches in which customer data may have been compromised – a regulation U.S. companies are subject to. Since many respondents indicated that they would disclose breaches only when legally required to do so, many security breaches will likely remain undisclosed unless these regulations change.

Reported Total Types of Breaches on the Decline

One interesting trend this year has been a decline in the total average number of types of breaches reported by respondents. This year, the average respondent reported 5.8 types of breaches resulting in incidents, compared to 6.7 last year (a 16% decline).

IT security breaches can take many forms. In 2009, the top five types of security breaches experienced by respondents included viruses, SPAM, spyware, security policy violations and phishing.

Figure 7 - Willingness to Disclose Breaches (2003 - 2009)



n=75 (2003); n=112 (2004); n=100 (2005); n=99 (2006); n=97 (2007); n=99(2008); n=99 (2009)

The breaches that were less likely to be reported this year than last year include the following:

- » End Point Security (reported by 26% of respondents this year, down from 52% last year)
- » SPAM (down 17% to 82%)
- » Theft of Sensitive Information (down 13% to 10%)
- » Phishing (down 13% to 59%)
- » Denial of Service Attacks (down 12% to 31%)

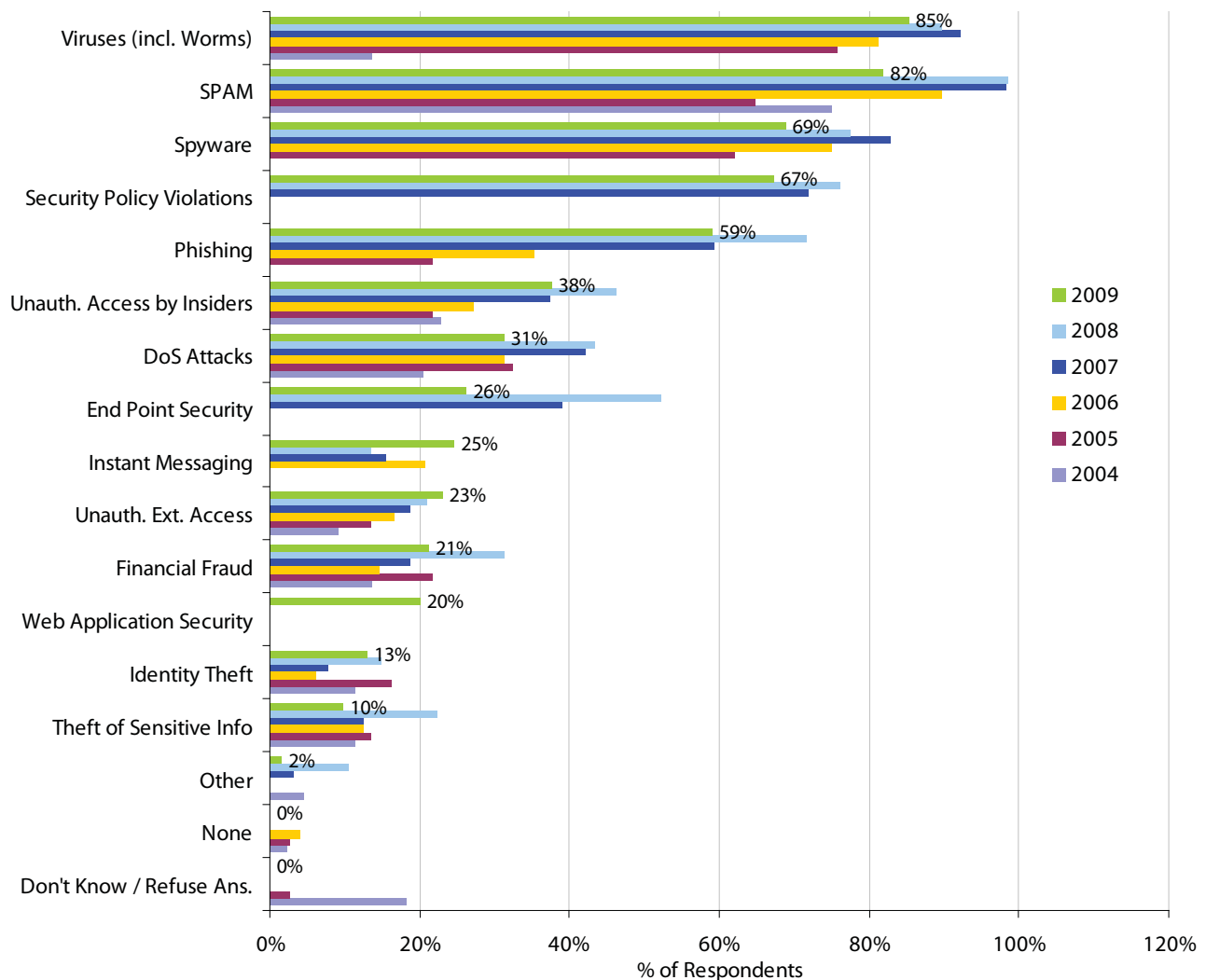
These declines are likely in part a result of increasingly proactive approaches to IT security. In addition, they may have been helped by the continued focus on the importance of policies, which are key to preventing certain types of breaches, such as incidents related to end point security or phishing.

One interesting increase this year has been the rise in reported incidents due to instant messaging, up from 13% in 2008 to 25% this year. This rise represents a reversal of a previous trend – incidents relating to instant messaging had fallen from 21% in 2006. This rise could be due in part to a more complacent approach to instant messaging due to the declining trend in previous years and the relatively low ranking of instant messaging on the list of concerns: this year, only 2% of companies put instant messaging among their top three concerns.

Web application security was added to the list of threats this year, after being identified last year as a significant new threat. In 2008, a study found that approximately 70% of web applications had critical security vulnerabilities⁷, indicating that organizations were not yet fully prepared to deal with this threat. In fact, as many as 20% of respondents this year reported having had a breach related to web application security.

⁷ Jackson, William. Studies find Web sites rife with unpatched vulnerabilities. Available at: <http://www.gcn.com/online/vol1_no1/47033-1.html?topic=security>

Figure 8 - Security Breaches Experienced (2004 - 2009)



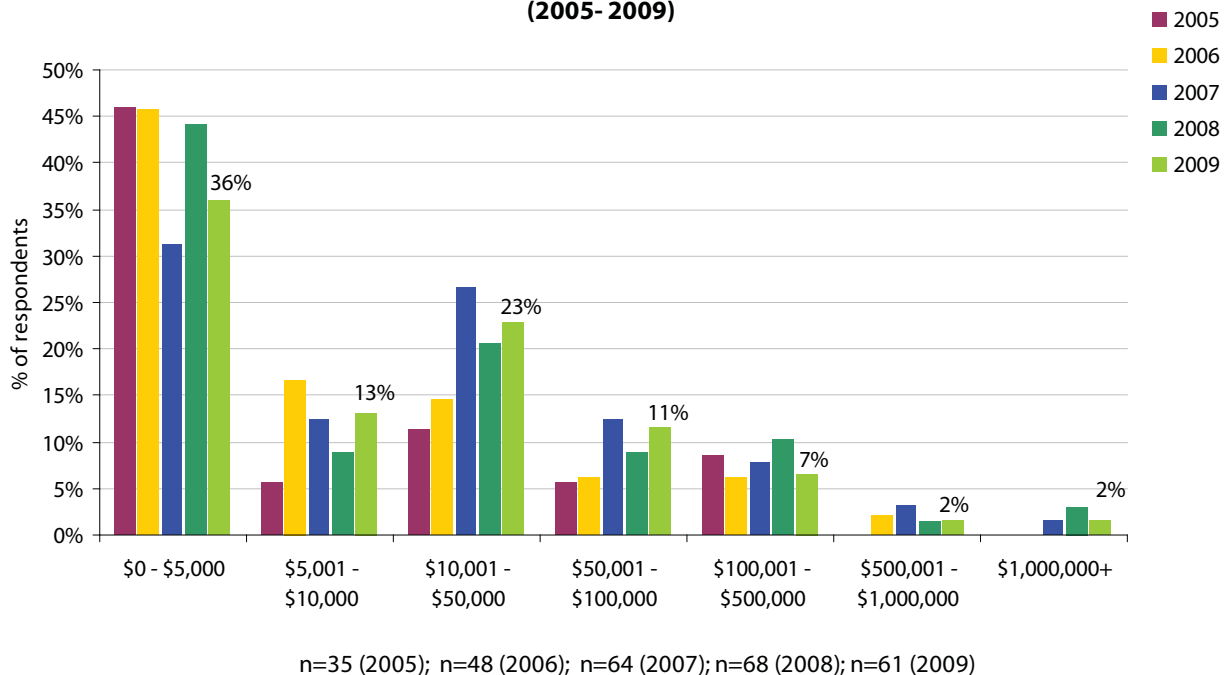
n=44 (2004); n=37 (2005); n=48 (2006); n=64 (2007); n=67 (2008); n=61 (2009)

Growth in Annual Spending on Breaches is in the Middle of the Cost Spectrum

There was a significant decline in the proportion of respondents that reported spending \$0-\$5,000 on breaches this year, from 44% to 36%. This is offset by an increase of 9% in the proportion of companies that reported spending \$5,001 - \$100,000 on breaches, while there has been a 5% decline in the proportion of respondents reporting more than \$100,000 in costs relating to breaches.

Last year, the growth was at the top and bottom of the cost spectrums. This year, the opposite occurred, with fewer companies reporting truly large expenses and a reduction in the proportion of companies that had few or no costs due to breaches. This may be due to some complacency on the part of companies that previously had very few breach-related expenses, which is consistent with a reduction in the deployment of some technologies which were also reported this year. At the same time, the reduction at the top of the cost spectrum is encouraging, and could be due to improved security in some organizations, possibly as a result of a more proactive approach.

Figure 9 - Estimated Total Annual Cost to Resolve Security Breaches (2005- 2009)



Companies Considering More Costs From Breaches This Year

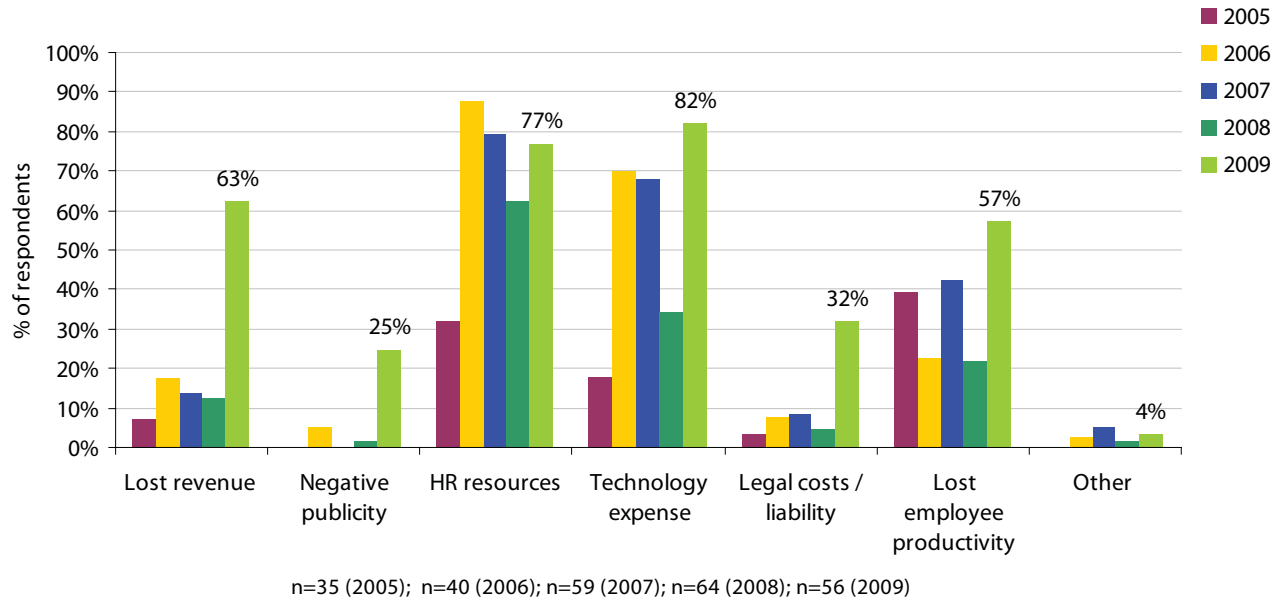
When asked what categories comprised the costs they incurred as a result of IT security breaches, the majority of respondents cited technology expense (82% of organizations), human resources (77%), lost revenue (63%) and lost employee productivity (57%). This represents a considerable change from last year: human resources is no longer the main reported cost and the number of categories respondents reported considering has risen significantly. The change in the proportion of companies including the following expenses in their estimates is:

- » Lost revenue (up from 13% to 63%)
- » Negative publicity (up from 2% to 25%)
- » Human resources (up from 63% to 77%)
- » Technology expenses (up from 34% to 82%)
- » Legal costs (up from 5% to 32%)
- » Lost employee productivity (up from 22% to 57%)

These results are surprising: last year, it appeared that companies continued to underestimate the true cost of security breaches and tended to classify important costs as overhead instead of measuring them as a component of IT security vulnerabilities. In addition, the relatively small change in the cost of breaches detailed above shows that this tendency did not necessarily subside this year.

While there were notable increases in all cost areas compared to previous years, the relatively stable total costs reported above show that organizations tend to overlook or underestimate certain costs, as previous years' results also indicated. It is apparent from this divergence that, while many respondents have the intention of recording a full spectrum of costs, actual recorded costs underestimate the relevant expenses in some categories, in particular lost revenue, negative publicity, and lost employee productivity.

Figure 10 - Primary Costs Caused by Security Breaches



Canada's Diverse Threatscape Continues to be Financially Motivated

Threats to IT security can take many forms, including

- » viruses, worms and blended threats;
- » external unauthorized access by hackers and crackers;
- » unauthorized activities by insiders (intentional and unintentional);
- » phishing (e-mail based attempts to fraudulently gain personal information);
- » pharming (use of malicious code to direct users to fraudulent websites without their knowledge);
- » denial of service attacks ("DoS"); and
- » SPAM, spyware and adware, among others.

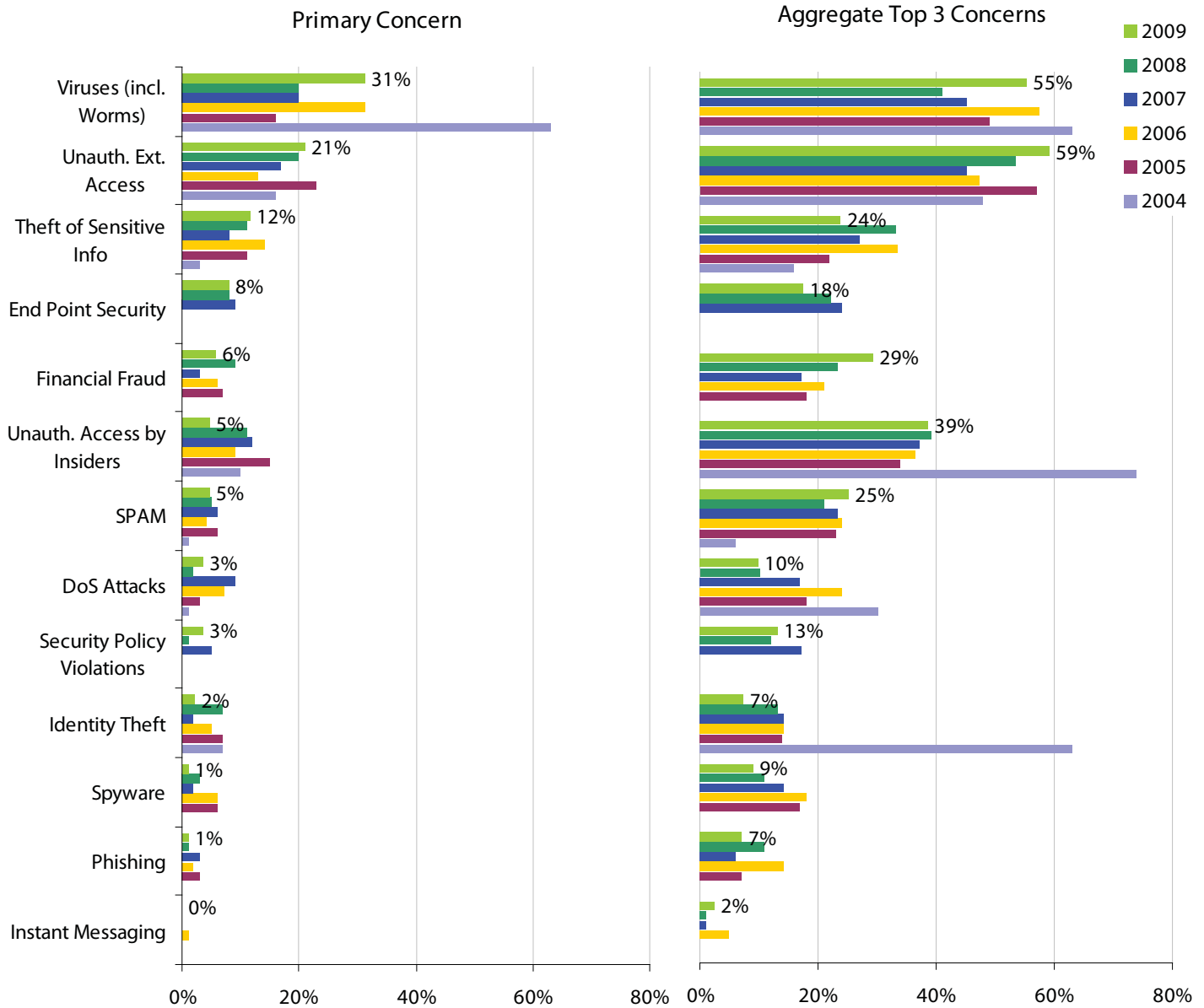
The threats to IT security are varied and ever-changing, in an age of a mature underground economy with global reach and the ability to quickly adapt their approaches. Symantec's recent Internet Security Threat reports have noted a trend toward web-based attacks, end-user targeting, and an increase in activities with the goal of financial gain.

The four most significant concerns among Canadian IT executives are viruses (the #1 concern for 31% of respondents), unauthorized external access (21%), theft of sensitive information (12%), and end-point security (8%). The biggest year-over-year this year occurred in concern about viruses: 57% more respondents listed viruses as their top concern this year than last year. Three of these top four concerns are due to financially motivated attacks.

The year-over-year changes in threats that companies list among their Top 3 concerns reveal that organizations are increasingly concerned about not only financial fraud, but also some of the categories they had become complacent about over the past few years, such as Viruses and SPAM. The greatest increases have occurred in the percentage of companies naming the following threats among their Top 3 IT Security concerns:

- » Viruses (+34%)
- » Financial fraud (+27%)
- » SPAM (+18%)
- » Security policy violations (+7%)

**Figure 11 - Ranking of Threats
(2004 - 2009)**



n=108 (2004); n=99 (2005); n=99 (2006); n=100 (2007); n=100 (2008); n=90 (2009)

On the other hand, this year organizations are less concerned about:

- » Identity theft (-45%)
- » Phishing (-36%)
- » Theft of sensitive information (-28%)
- » End point security (-21%)

This likely represents an increased level of confidence among respondents about their ability to cope with those types of attacks.

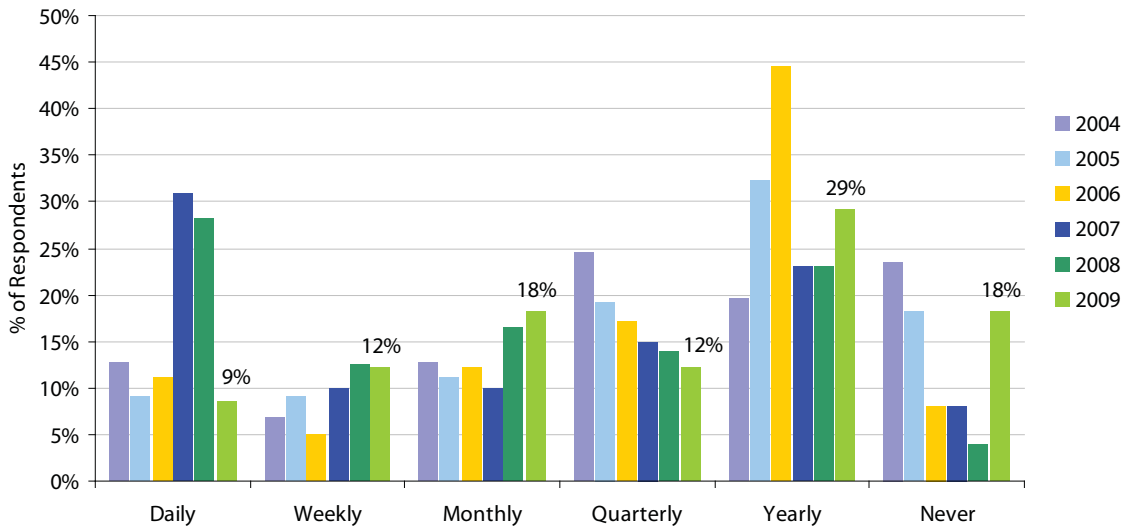
Viruses

Concern About Viruses Continues to Rise, Threat Management Mostly Successful

This year, viruses were the most common form of attack experienced by respondents (up from a ranking of second last year), having been experienced by 85% of respondents. Viruses also was once again one of the top two concerns for organizations, ranked among the top three concerns by 55% of respondents and ranked as the #1 concern by 31% of respondents (more than any other single threat). It appears that companies' concern about viruses has grown this year, with a larger proportion listing them either as the top concern or one of the top three IT security concerns for their organizations. The potential costs of remediation in case of a network-wide outbreak are high, and the ability of viruses and other malware to disrupt operations and continually change are some of the reasons behind the high levels of concern about this pernicious threat.

This year, the prevalence and frequency of virus infections both declined slightly. Infections were reported by 85% of respondents, down from 90% last year. In addition, the proportion of organizations reporting daily infections declined from 28% to just 9%, while the proportion of respondents reporting infections yearly or less than yearly increased by 20%.

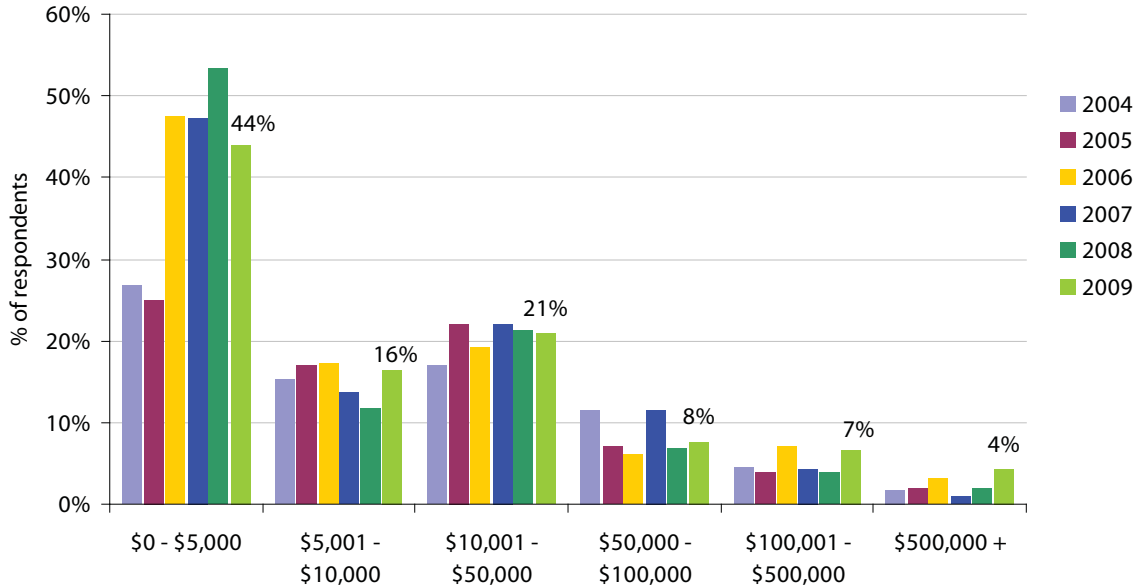
Figure 12 - Frequency of Virus Outbreaks (2004 - 2009)



n=102 (2004); n=99 (2005); n=99 (2006); n=100 (2007); n=103 (2008); n=82 (2009)

Unfortunately, although the prevalence of virus infections this year declined slightly in absolute terms, it appears that the virulence of those infections is on the rise, since the cost to treat virus infections has increased. The proportion of respondents that reported an average cost per outbreak of less than \$5,000 declined from 53% to 44%. This decline was offset by an increase from 12% to 16% in the \$5,001 - \$10,000 category and an increase from 13% to 19% in the proportion of respondents reporting average costs of \$50,000 or more.

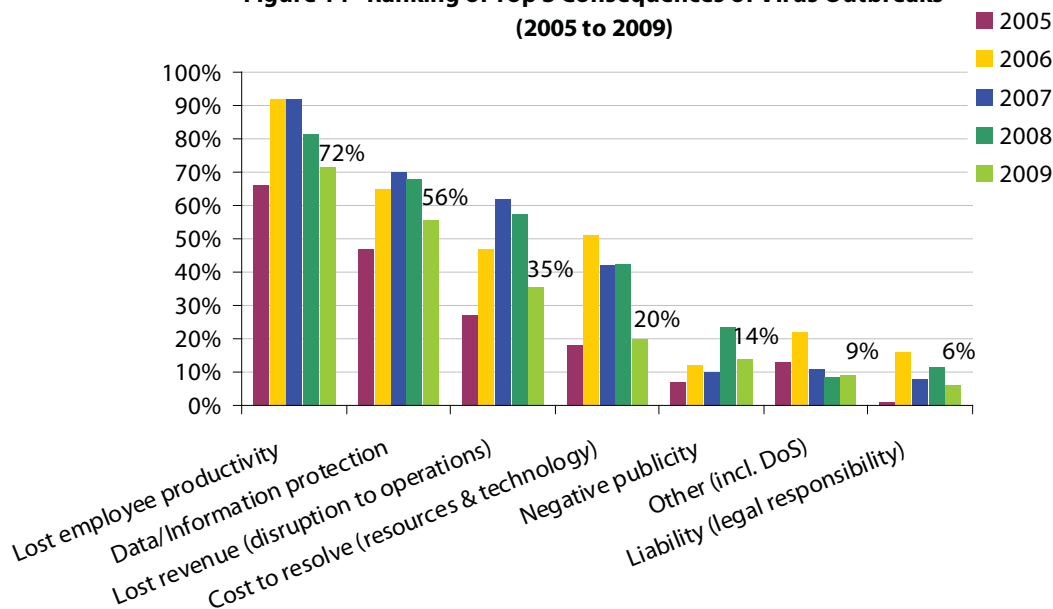
Figure 13 - Cost to Resolve a Virus Outbreak



n=112 (2004); n=100 (2005); n=99 (2006); n=95 (2007); n=103 (2008); n=91 (2009)

This year, the perceived threats from virus outbreaks are similar to previous years' results, with lost employee productivity, data/information protection, lost revenue due to disruption to business operations and cost of resolution once again forming the top 4 concerns due to virus outbreaks for IT managers. This year, respondents were more likely to list one or two main concerns instead of their top 3 concerns, resulting in lower absolute percentages in most categories. This is consistent with this year's tendency among respondents to focus on key issues, rather than try to solve and prevent all the possible threats.

Figure 14 - Ranking of Top 3 Consequences of Virus Outbreaks (2005 to 2009)



n=100 (2005) n=100 (2006) n= 100 (2007) n=103 (2008); n=99 (2009)

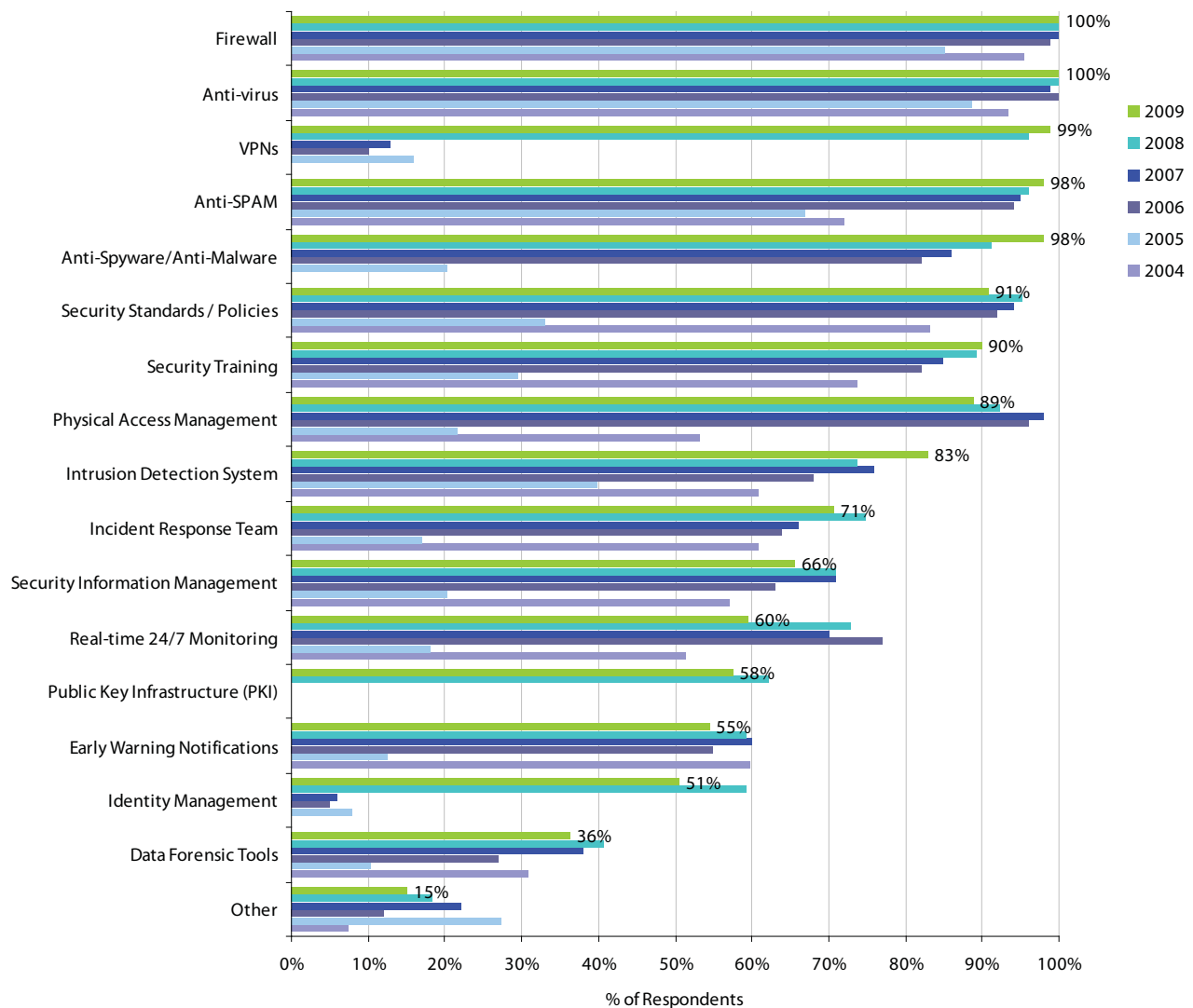
Preparation, Prevention and Management

IT Security Inventory Continues to Stabilize

Once again, the 2009 responses showed that the majority of essential security measures have been adopted by most large organizations. As figure 15 shows, virus protection and firewalls have been adopted by 100% of respondents. Other areas of growth in 2009 include VPNs, anti-SPAM, anti-spyware and intrusion detection and prevention software.

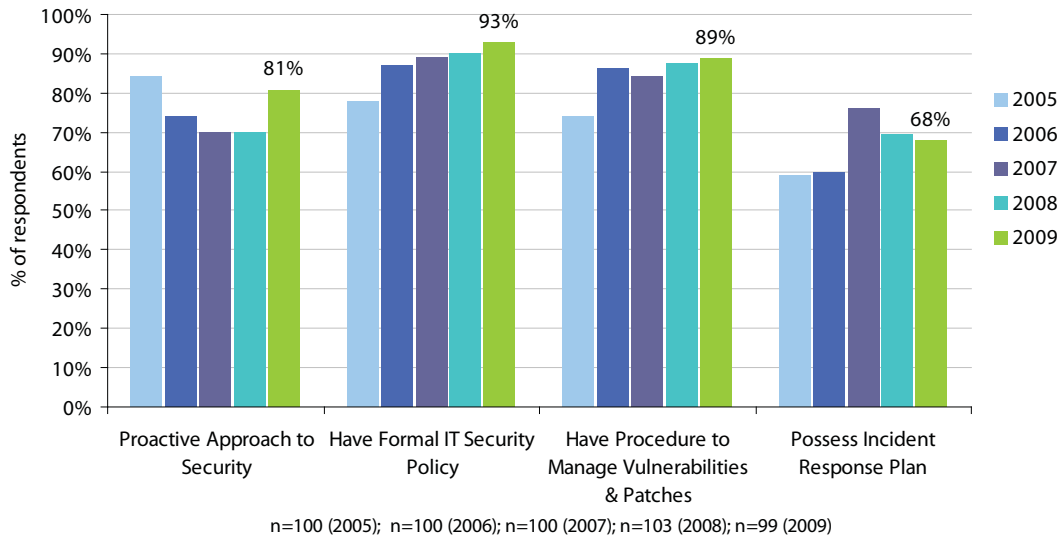
Several categories experienced a slight reported decline this year, including early warning notifications, identity management, public key infrastructure and real-time 24/7 monitoring. This is a reversal of the trend toward wider adoption seen over the past several years, and could be due to differences in the survey sample, as well as to some prioritization due to budgetary constraints over the past year. Several respondents indicated that they felt they had deployed the tools which were essential for their organizations, and that additional tools were not necessary at this time.

Figure 15 - IT Security Inventory



n=112 (2004); n=94 (2005); n=100 (2006); n=100 (2007); n=103 (2008); n=99 (2009)

Figure 16 - IT Security Policy & Processes



Adoption of Key Security Measures is Stagnating

Over the past several years, respondents have generally built up their security arsenals and ensured that they were taking many important measures to ensure the security of their networks. This has resulted in relatively high penetration of IT security processes such as formal policies (93% in 2009), procedures to manage vulnerabilities and patches (89%) and incident response plans (68%). However, while there has been an increase in the proportion of respondents who considered themselves as having a proactive approach to security, there has been stagnation in these other measures, and even a decline in the penetration of incidence response plans.

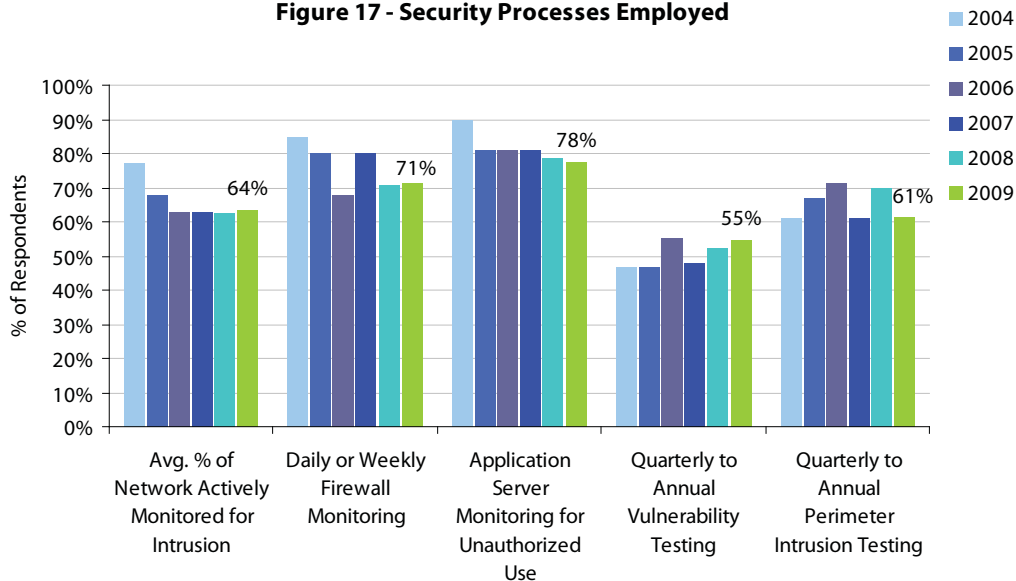
The total penetration of these measures is, however, relatively high, and reflects an understanding of the threats large organizations face. In addition, the proactive approach that companies are taking seems to be paying off, with only 19% of companies that identified themselves as proactive more concerned about security this year (compared to 35% last year, and 47% of companies that identified themselves as reactive).

The adoption of tactical initiatives, including network, firewall, and application server monitoring for intrusions, has also been fairly stable in 2009, with slight increases or declines across all the categories. Adoption of proactive measures has continued to be strong, with 86% of organizations running regular vulnerability assessment scans and 76% running regular perimeter penetration testing.

Canadian companies' implementation of proactive measures in 2009 can be summarized as follows:

- » **Active intrusion monitoring** – Overall, 64% of a network is actively monitored for intrusions, up from 63% last year but down from a high of 77% in 2004. The adoption of these technologies appears to have stagnated in the past six years.
- » **Firewall monitoring** – Firewalls are an essential component of an organization's security strategy and a company's first line of defense against intrusions. This year, 71% of companies reported daily or weekly firewall monitoring (the same as last year and down 11% since 2007). However, another 15% of respondents monitored their firewalls monthly or quarterly.
- » **Application server monitoring** – The adoption of this important security tool has continued to stagnate in 2009. This year, 22% of respondents did not monitor their application servers.
- » **Vulnerability Assessments** – This year, 86% of respondents ran regular vulnerability assessment scans, up from 83% last year. Of those, 31% performed them daily, weekly or monthly, while 31% performed them quarterly and 23% performed them only annually.

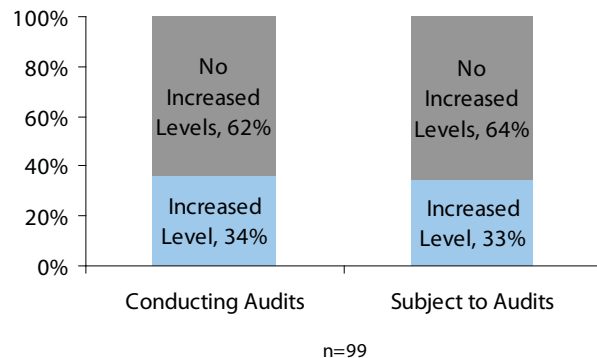
Figure 17 - Security Processes Employed



n= 93 to 112 depending on question and year

- » **Perimeter penetration testing** – This year, only 76% of companies conducted regular penetration testing on their infrastructure, while an alarming 12% of respondents reported never conducting penetration testing. Only 14% of respondents conducted perimeter penetration testing daily, weekly or monthly.
- » **Incident Response Plans** - One disconcerting trend that has surfaced in the past two years has been the reduced adoption of incident response plans among respondents. In 2009, only 68% of respondents reported having an incident response plan, 2% fewer than in 2008 and 10% fewer than in 2007.
- » **Formal procedure to manage and implement patches** – Considering that 80% of vulnerabilities in 2008 were classified as “easily exploitable” (up from 74% in 2007)⁸ and that time to patch is significantly longer than time to exploit, a patch management procedure is crucial for large enterprises. In fact, 89% of respondents had a formal patch management procedure in place, up from 87% in 2008.
- » **Partner audits:** This year, only 34% of respondents reported conducting more security/privacy audits with partners, while just 33% reported being subjected to an increased level of audits. This rate of growth is significantly lower than last year’s (52% and 43%, respectively), which is lower than the growth in 2007. It appears that the move toward greater audits has leveled off in 2009, with the majority of companies satisfied with their existing procedures and not seeing partner audits as a priority area.

Figure 18- Security / Privacy Audit Activity (2009)



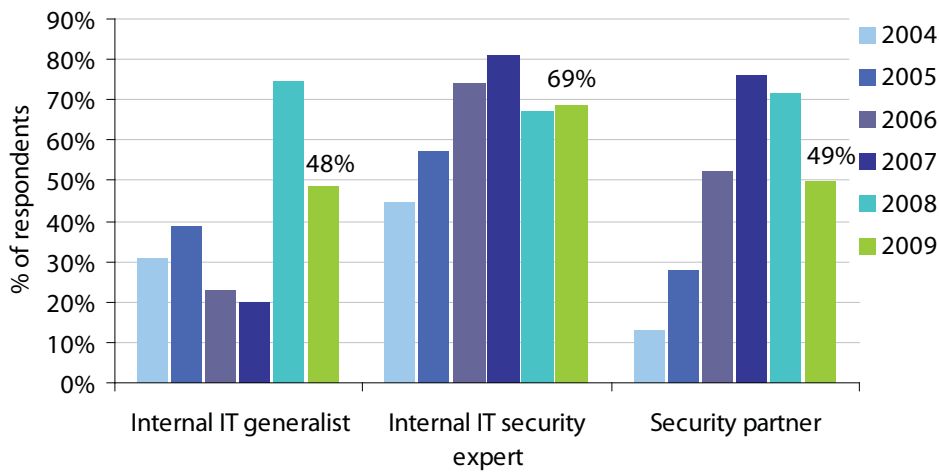
While adoption of all of the security measures discussed above is relatively high, with the majority of respondents having implemented many key processes, the stagnating adoption of many measures over the past five years is disconcerting. There are more reasons than ever for companies to be concerned as cyber-criminals continue to gain in sophistication, and robust security processes are essential for large organizations.

8 “Symantec Internet Security Threat Report: Trends for 2008”. Vol. XIV, Published April 2009.

Resourcing and Outsourcing

This year, a slow economy and the resulting budgetary pressures have significantly affected respondents' resourcing and outsourcing strategies. One trend in IT management among Canadian companies that has reversed this year is the adoption of Chief Security Officers (CSO) and Chief Privacy Officers (CPO). The reported use of both among respondents decreased significantly this year - only 25% of organizations reported having a CSO (down from 31% last year and similar to 24% in 2007), while just 19% reported having a CPO (down from 34% last year and 28% in 2007).

Figure 19 - IT Security HR Approaches



n=100 (2004); n=100 (2005); n=100 (2006); n=100 (2007); n=103 (2008); n=99 (2009)

This year, the most popular approach to solving IT security problems has been to use an internal IT Security expert or team of experts, used by 69% of organizations. The use of internal IT generalists as a primary approach dropped by 26% to just 48% this year, although this still represents a significant increase from just 20% in 2007. The preference toward IT security experts this year is consistent with an increasing awareness of the importance of IT security, even at a time of budgetary cutbacks.

The financial constraints faced by companies this year were certainly reflected in the use of security partners as a primary approach to IT security issues, which declined from 72% to 49% of respondents this year. Interestingly, the trend toward a diminishing proportion of services delivered by partners reversed this year, increasing to 30% of security delivered to clients that used outsourcing. While the 2005-2008 period saw an increase in the proportion of respondents using outsourcing to deliver a small percentage (0-25%) of IT security services, this year these "light" users of outsourcing appear to have switched some of those services to their internal teams. In addition, more respondents used a single partner this year, indicating that companies are focusing their IT spend on essential services from a few trusted providers, which is consistent with a more economical approach. Satisfaction with the performance of these outsourcers also went up this year, from 7.31/10 to 7.94/10, pointing to an increased focus on only those vendors and services where the demonstrated value was clear.

Figure 20 - Outsourcing Practices
% of Security Delivered by Business Partners

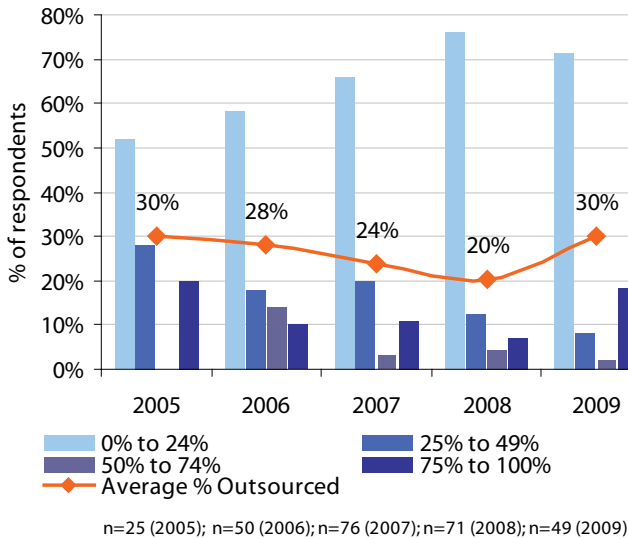
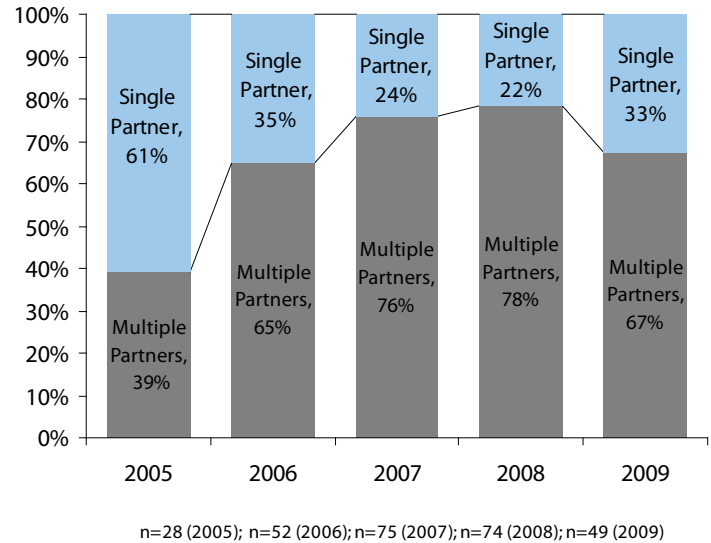


Figure 21 - Outsourcing Practices
Multiple Partner Use

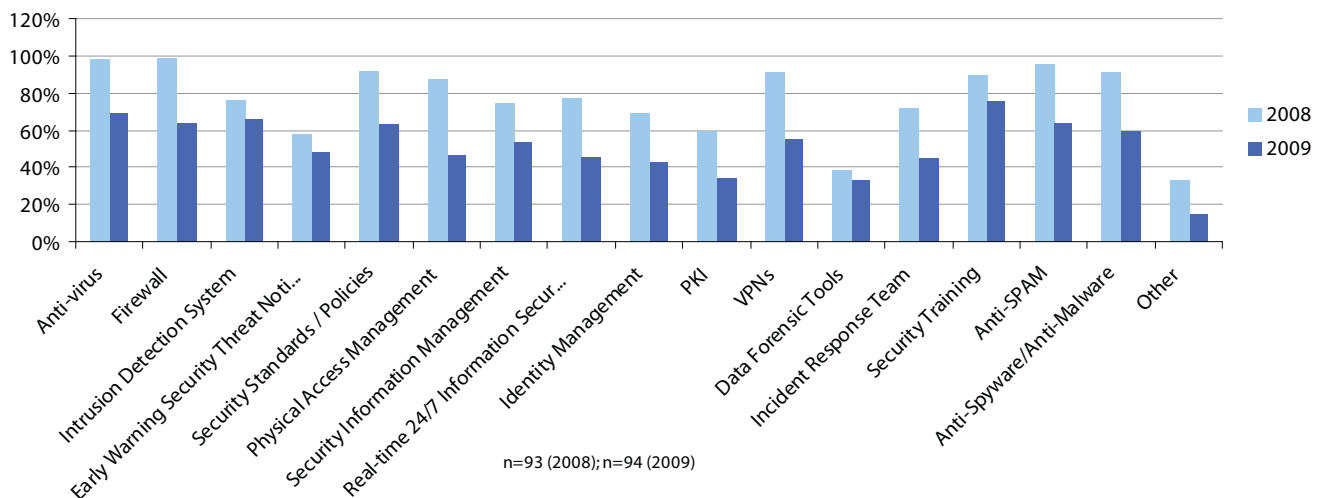


Investment Trends and Plans

Spending Plans are Down Again as Companies Continue to Prioritize

Last year's study found that spending plans were down in most areas of IT security; in fact, spending did decline last year. This year, again, respondents have indicated that their investment plans are in decline across the board. Figure 22 shows the proportion of respondents that indicated planned financial investments in each IT security area over the following year. The trend clearly points toward conservative spending plans. The greatest declines are in physical access management, VPNs, firewalls, incident response teams and identity management.

Figure 22 - IT Security Investment Plans (2008-2009)

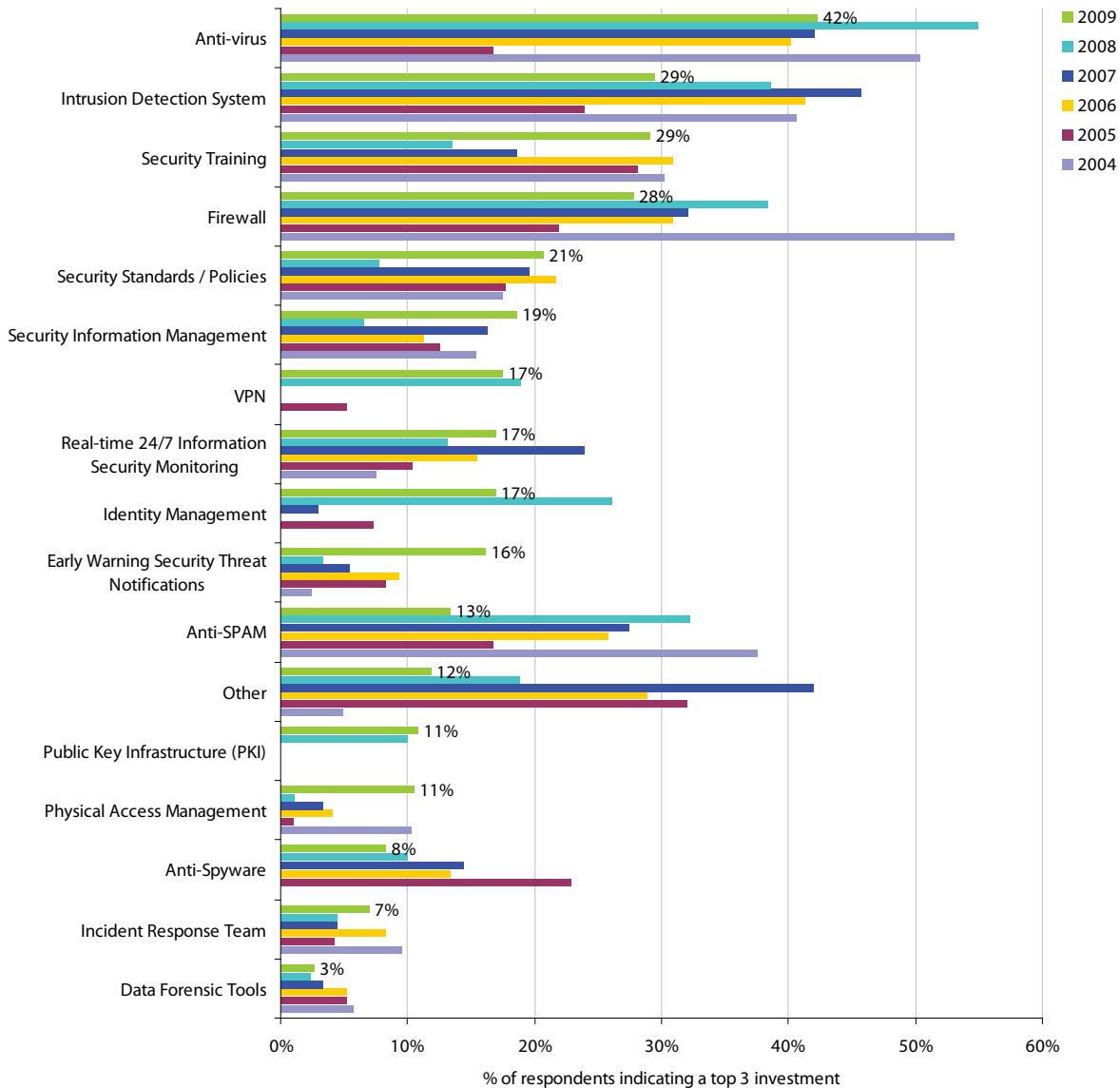


This decline in spending plans is related in part to a relatively mature security arsenal in many respondent organizations and an increasing need to prioritize spending on those areas where a return is easily justifiable, or those in which current needs are significant. Figure 23 shows the spending priorities of respondents, tracking the Top 3 planned investments from 2004 to 2009.

This year, there have been increases in the prioritization of Security Training, Security Standards/Policies, Early Warning Security Threat Notifications, Security Information Management and Physical Access Management. The areas which declined in importance include Anti-SPAM, Anti-virus, Firewall, and Identity Management; most of these are areas which already have a very high penetration rate among respondents.

The industries that planned to invest in the largest number of different technologies included Agriculture, Natural Resources, Telecommunication, Education and Utilities. The industries that reported planning to focus on fewer targeted investments included High-Tech and Financial Services.

**Figure 23 - IT Security Investment Plans (Top 3)
(2004 -2009)**

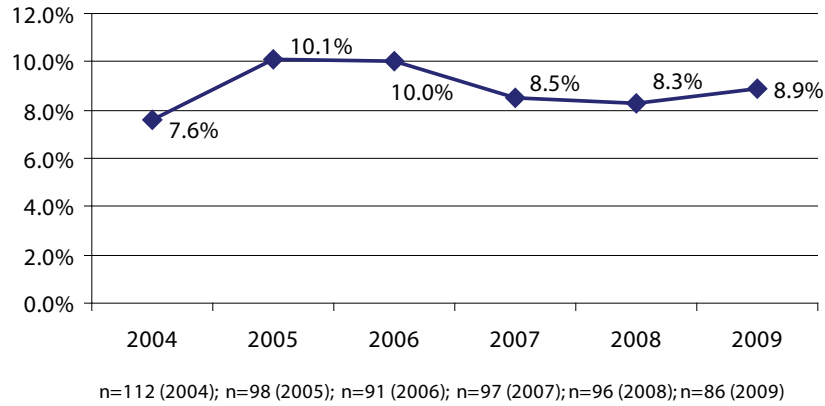


n=101 (2004); n=96 (2005); n=96 (2006); n=95 (2007); n=93 (2008); n=94 (2009)

Budget Trends

In 2009, the proportion of total IT spending for Canadian companies on IT security has increased from 8.3% to 8.9%, which is still a decline from a high of 10.1% in 2005. The median spending is the same this year at 5%, where it has been in 2004, 2006 and 2007 and 2008 (with a brief increase to 6% in 2005).

Figure 24 - IT Security Spend as a % of Total IT Spending



As shown in figure 25, the proportion of companies spending less than 4% on security rose to 36% this year, along with the proportion of companies spending 20-29% of their budget on security (up from 3% to 13% this year). The declines occurred in the middle, with fewer organizations spending between 5 and 19% of their IT budgets on IT security. The industries that spent the largest proportions of their IT budgets on security included insurance, natural resources, manufacturing and financial services.

Figure 25 - Proportion of IT Spend on Security Products & Services (2004 to 2009)

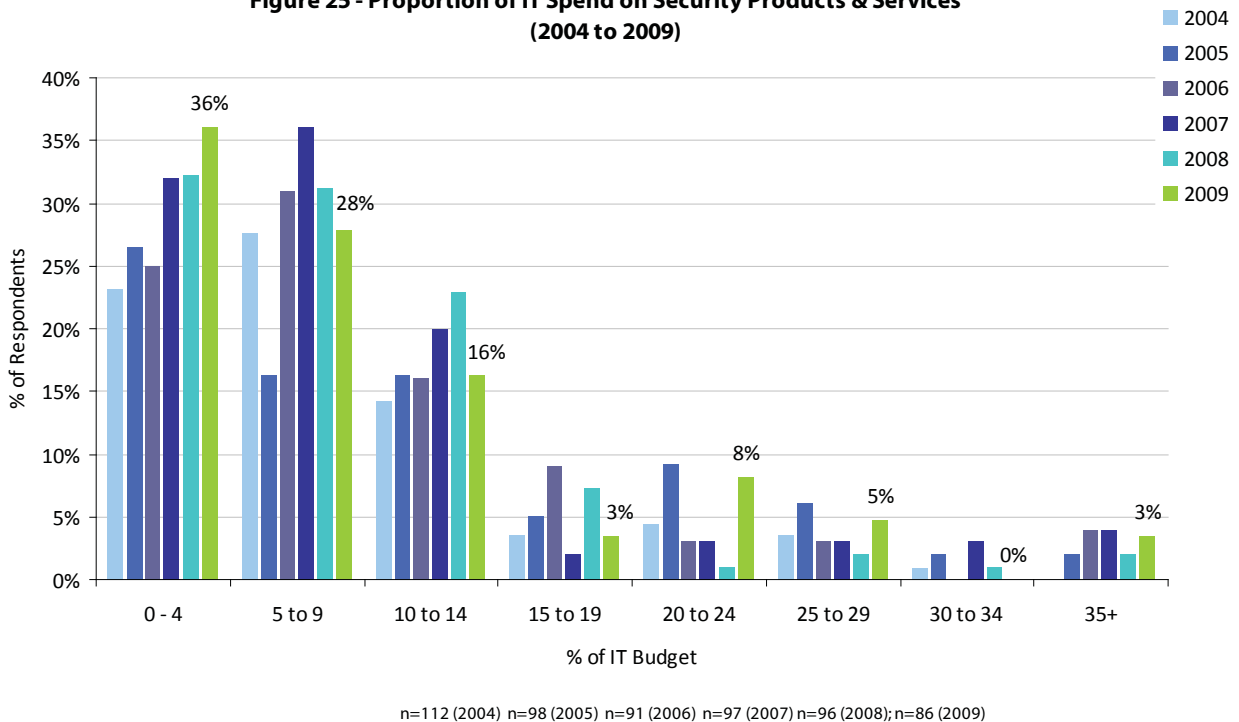
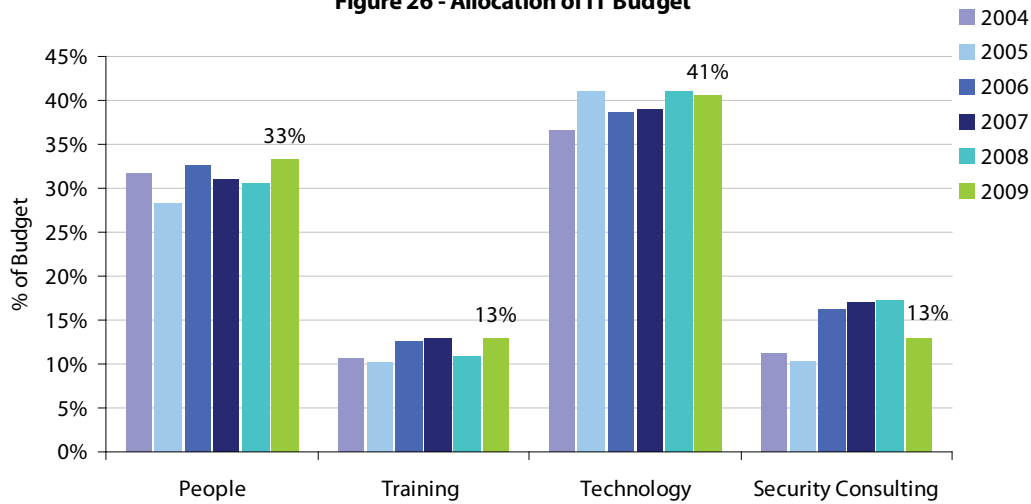


Figure 26 - Allocation of IT Budget



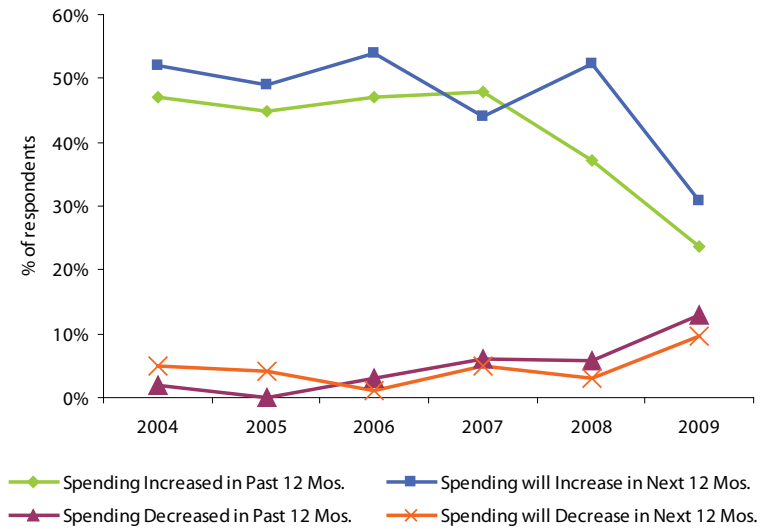
n=82 (2004); n=91 (2005); n=95 (2006); n=98 (2007); n=100 (2008); n=89 (2009)

The allocation of respondents' IT Security budgets has remained relatively stable this year. As expected, respondents reported spending less on external consulting, with corresponding increases in spending on People and Training. Technology costs have stayed at 41% this year, once again representing the single largest expenditure.

The stability of the Technology spending as a percentage of the total security budget may seem strange, considering the reduced spending plans reported both this year and last year. However, these expenditures must be seen in the context of overall budgets which have been reduced for many respondents this year. IT security managers' perception of security spending dropped precipitously in the past year, with a much lower percentage than usual reporting that spending increased in the past year (24% in 2009 vs. 37% in 2008 and 48% in 2007) and a significantly higher percentage reporting a spending decrease (13% in 2009 vs. 6% in 2008 and 2007).

This year's spending expectations are also more pessimistic than usual. Only 31% expect an increase in the next year, compared to 52% in 2008. In addition, 10% expect a decrease, up from just 3% in 2008. It is clear that the outlook for IT security budgets and expenditures is still grim as of the time of this study. However, it should also be noted that expectations are not perfect predictors of future spending.

Figure 27 - % Indicating Belief in Spending Increase / Decrease



n=106 (2004); n=99 (2005); n=100 (2006); n=100 (2007); n=103 (2008); n=93 (2009)

Conclusion

Every year, the challenges faced by Canadian IT security managers have grown, along with the creativity and determination of organized criminals determined to access their valuable data. Companies have had to deal with more attacks on their data each year, and have responded by building up their security toolkit to accomplish their #1 priority of keeping their data safe.

The threatscape has certainly grown more challenging this year; for instance, this year Symantec detected more vulnerabilities, more easily exploitable vulnerabilities, and more phishing hosts than ever before. In addition, IT managers have faced the challenge of reduced budgets, a result of the economic difficulties which have deeply affected our respondents this year. However, organizations have made do with the resources available to them, and have actually reported fewer incidents this year.

At the same time, however, several disconcerting trends have emerged. In particular, the adoption of key IT security tools, including network and application server monitoring and incident response plans, has stalled. In addition, the investment plans for the future have also dropped, due in part to anticipation of possible further budget cuts in the future. However, it is essential that organizations continue to implement these important tools when they are able to do so. Whether or not that happens depends in part on whether IT security regains its place near the top of the corporate priority list when the economy recovers. Considering that there are more threats than ever to organizations' networks and the consequences of a data breach on a massive scale can be dire, it is essential that IT security once again becomes an organizational priority.



About Branham Group Inc.

Branham Group is a leading industry analyst and strategic consulting firm servicing the global information technology marketplace. Branham Group assists information technology companies and related institutions in achieving market success through its custom consulting services (Planning, Marketing and Partnering), and through its multiclient research subscription programs (eHealth, Outsourcing and Green IT). Branham also produces an annual listing of the top information technology companies in Canada (www.branham300.com), tracks the Canadian Outsourcing industry (www.branhamoutsourcing.com) and monitors over 450 eHealth vendors.

For more information regarding Branham Group, please visit www.branhamgroup.com.

Branham Group Inc.

45 O'Connor Street, Suite 1150
Ottawa, ON
Canada • K1P 1A4
Tel: 613.745.2282
Fax: 613.745.4990
www.branhamgroup.com

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com. Symantec's Canadian operations are headquartered in Toronto with offices in Montreal, Ottawa, Calgary and Vancouver. For more information on Symantec products or current promotions, access Symantec's Canadian Web site at www.symantec.ca. Symantec is an active member of the Business Software Alliance (BSA).

Symantec Canada

3881 Steeles Avenue East, 4th Floor
Toronto, ON
Canada • M2H 3S7
Tel: 416.774.0000
Fax: 416.774.0001
www.symantec.ca