

# Symantec 2008

## Pulse of IT Security in Canada

### Volume VI

---

The annual Symantec Pulse of IT Security in Canada survey, now in its sixth 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 2008.

#### KEY FINDINGS

##### Importance of IT Security

- While all respondents articulate that IT Security is important, only 70% (vs. 82% last year) see it as a top 5 priority.
- The proportion of IT Security Managers more concerned with IT security compared to 12 months ago rose to 41% (vs. 34% in 2007). 6% are less concerned, although this is up from 4% last year.
- Data protection and reputational risks were the top concerns among respondents, due to the significant financial and brand erosion consequences of breaches. Lost revenue due to disruption of operations was the third most important driver this year (and the second last year), appearing among the top 3 priorities of 47% of companies surveyed.
- Approximately 1 in 3 companies have created positions of Chief Privacy Officer and Chief Security Officer, both up slightly from last year.

##### Coping with a diverse threatscape

- The most common reported security attacks comprise SPAM (99%), Viruses / Worms (90%), Spyware (78%) and Security Policy Violations (76%).
- The highest rates of growth this year occurred in Identity Theft (91% more companies experienced this breach in 2008 than in 2007), Theft of Sensitive Information (+79%), and Financial Fraud (+67%).
- The perceived risk of attack fell slightly from last year, but so too did the organizations' estimate of their ability to protect themselves from an attack.
- 67% of respondents claim to be willing to admit a security breach publicly, compared to 66% last year, up significantly from 41% in 2003.
- The annual cost of managing security breaches continues to be driven by HR costs, technology costs and lost employee productivity. However, the percentage of companies including each of these costs in their calculations declined in 2008.

##### Virus/Worm Infections

- Viruses are among the top two concerns of IT managers. Due to the increasing professionalization of hackers, however, viruses have lost some ground to external breaches in general this year.
- The reported frequency of virus outbreaks is on the rise: while the percentage reporting daily occurrences dropped slightly from 31% to 28%, the percentage reporting weekly or monthly infections increased from 20% to 30%.
- 53% of respondents estimate the cost to resolve a virus outbreak at less than \$5,000.
- IT security managers perceive lost employee productivity (82%), compromised data/information protection (68%), lost revenue (57%) and costs to resolve outbreaks (43%) as the greatest threats from virus outbreaks.

##### Approach to IT Security

- 70% of organizations report having a proactive approach to security, unchanged from last year.
- The trend toward employing IT specialists appears to have reversed this year: companies employing generalists increased from 20% to 75% this year, while use of specialists declined from 80% to 67%.
- 72% of respondents outsource some elements of their IT security. The average portion of IT security outsourced has declined steadily to 20% this year from 30% in 2005.
- The use of multiple partners continues to grow, with 78% employing multiple partners, up from 76% last year and 39% in 2005.

##### Investment in IT Security

- Among the top 3 investment plans for 2008-09, anti-virus (55%), intrusion detection (39%), and firewall investments (38%) ranked highest.
- Median spending remains static at 5% of total IT budgets. 63% of respondents indicate that they spend less than 10% of total IT spend on security.
- Technology (39%) and internal staff (31%) represent the bulk of IT spend.

## FOREWORD

---

If the word “Focus” captured the developments in last year’s IT Security approach among Canadian companies, this year’s trends point toward **Complacency**.

There is no doubt that the market has matured. During the past four years, companies have made substantial investments in IT Security, and more companies than ever have deployed key technologies to protect their digital assets and established internal policies for preventing and managing threats. However, this year companies reported that their spending on IT security has decreased in the past twelve months and that more companies than ever are planning to invest in only core technologies in the upcoming year. While large organizations are reporting more security breaches than ever before, the proportion taking a proactive approach has stagnated at 70%. Despite more breaches, companies consider themselves less vulnerable than they did last year, although they also admit to feeling less prepared to deal with threats as well.

IT professionals face more threats than ever this year, as they find themselves in a threatscape increasingly characterized by international and professional cyber-criminals intent on committing fraud and gaining access to customer data – a breach that can alienate customers, send share prices plunging, and possibly find unprepared companies facing significant financial penalties. Cyber-criminals are becoming more sophisticated in their quest for private financial information, focusing on end-user attacks, on the web as an increasingly effective vector of malware, and on attacking popular web 2.0 technologies and web applications which have all-too-exploitable security flaws. In the second half of 2007, the Symantec Internet Security Threat Report revealed several disturbing trends:

- » The number of phishing hosts detected increased 167% from the first half of 2007 and a 559% increase from the first half of 2006;
- » Threats to confidential information made up 68% of the top 50 malicious code samples;
- » Malicious activity has become increasingly web-based;
- » Of the 11,253 site-specific cross-scripting vulnerabilities documented by Symantec, only 473 had been patched and the average patch development time was 52 days.

While companies have a long way to go, this study has demonstrated the significant progress that has been made over the last five years. Canadian organizations’ view of security has become more strategic and more proactive. Companies have become much more willing to admit when they have experienced security breaches: two-thirds are now willing to do so, compared to just 41% in 2003. In addition, the adoption of many security solutions has been very encouraging: for instance, only 20% of companies had anti-malware protection in 2005, whereas 91% reported having it in 2008.

Clearly, significant progress has been made, but each year new and more sophisticated threats face large organizations. As companies adopt innovations like the use of end-point devices and web applications, they must remain vigilant about threats and proactive in their prevention. The cost of complacency – both financial and reputational – is too great not to do so.

## INTRODUCTION

The sixth annual Symantec *Pulse of IT Security in Canada* survey was conducted in June and July 2008 to gain insight into Canadian enterprise IT security issues and trends.

One hundred and three 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.<sup>1</sup>

### SURVEY DATA

**Targets:**

Canadian enterprises  
Revenues > \$50 million

**Respondents:**

Senior IT managers and executives  
responsible for enterprise security

**Respondent Type:**

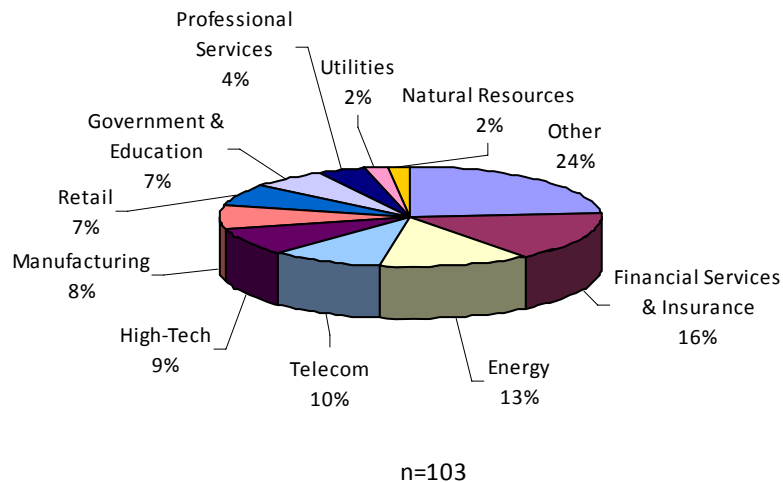
VP IT/IS, CIOs, Security Managers,  
Directors of IT Security, IT Security  
Architects, etc.

**Timeframe:** June – July 2008

**Total Respondents:** 103

This year's respondents represent a diverse cross-section of the Canadian economy, with 38% of the respondents coming from the Financial Services, Insurance, Energy and Telecommunications sectors.<sup>2</sup>

Figure 1 - Respondent Industries 2008



This report summarizes key findings from the survey and compares this year's responses to those from 2003-2007 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.

<sup>1</sup> The surveys conducted in 2005 - 2008 all contained the same questions, but differ from 2003 and 2004 in some elements, precluding comparison on these elements.

<sup>2</sup> With a total sample of 103 respondents in 2008, sectoral data is not deemed statistically relevant, however may provide indicators of new or ongoing developments in those segments.

## IMPORTANCE OF ENTERPRISE SECURITY

During the 2007-2008 period, the number of highly publicized security breaches has declined, lulling some organizations into a false sense of security. While organizations have certainly already made substantial investments into security which have paid off in many cases, respondents appear to be increasingly complacent about the possibility of an attack.

Despite less mainstream media coverage, security professionals have noted a number of disturbing trends in 2008. For instance,

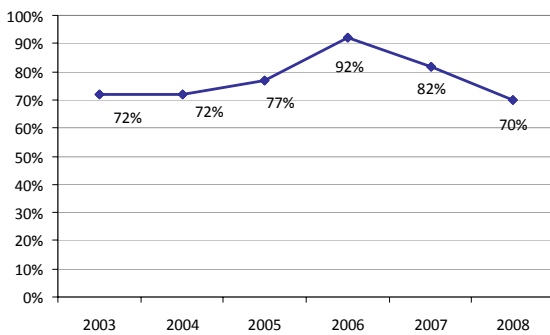
- » More large-scale fraud and criminal behavior has an international aspect to it;<sup>3</sup>
- » The web appears to have overtaken spam as a driver of malware infections;<sup>4</sup> and
- » Approximately 70% of web applications, which are becoming an increasingly popular way to deliver software, were found to have critical security vulnerabilities in a 2008 study.<sup>5</sup>

In the past, there has been a consistent shift where IT security has moved from more of an IT domain to one that is strategic in nature, garnering the attention of senior executives in boardroom discussions. In 2008 however, it appears that this shift has slowed.

### IT SECURITY CONCERN RISES WHILE PRIORITY LEVEL DROPS IN A MATURING INDUSTRY

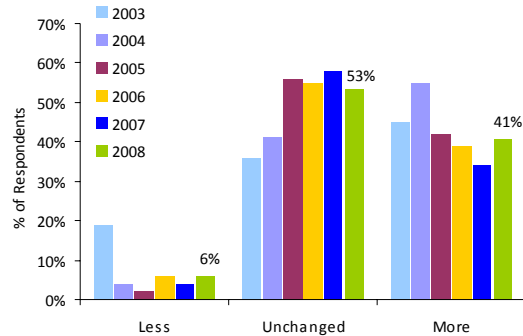
While all organizations surveyed this year considered IT security important, the percentage of organizations that rank IT Security among the top 5 corporate priorities has declined to an all-time low of 70%. This represents a continuation of the trend reversal that began last year: while Security's presence among the top 5 corporate priorities rose 20% during the 2003-2006 period, it diminished 10% and 12% in 2007 and 2008, respectively.

Figure 2 - % Indicating Security as a Top 5 Priority (2003-2008)



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

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



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

<sup>3</sup> Purdue Expert Says Consumers Absorb Cybercrime Costs, Newsroom, <<http://www.insideindianabusiness.com/newsitem.asp?ID=31150>>

<sup>4</sup> Symantec Internet Security Threat Report, Trends for July-December 07, Volume XIII

<sup>5</sup> Jackson, William. *Studies find Web sites rife with unpatched vulnerabilities*. Available at: <[http://www.gcn.com/online/vol1\\_no1/47033-1.html?topic=security](http://www.gcn.com/online/vol1_no1/47033-1.html?topic=security)>

This significant drop points to a certain level of complacency. However, it does not mean that organizations are less concerned about security – on the contrary, the percentage of respondents who are more concerned about security this year than they were 12 months ago rose from 34% to 41% this year. Rather, it appears that the IT security field has matured and more organizations feel that IT security is an ongoing, “fact-of-life” concern that must be managed consistently, not as a special strategic focus in any given year.

Naturally, IT vulnerabilities pose a greater threat to organizations in some industries than to others. Industries which are most likely to rank IT Security among Top 5 Priorities include government, insurance, high tech, education and retail.

Companies from the financial, education and retail industries were most likely to be more concerned about IT security this year than 12 months ago. On the other hand, the high tech and manufacturing industries experienced the biggest drops in levels of concern.

### **PROACTIVE COMPANIES WORRY LESS THIS YEAR; 30% REMAIN REACTIVE**

Among companies which did not rank IT Security as a Top 5 priority, 61% took a proactive approach to security. Interestingly, among companies which ranked it in the Top 5, only 74% took a proactive approach. While this is certainly an improvement, it is still disconcerting that 26% of companies which consider IT security to be a Top 5 corporate priority do not take a proactive approach to its management.

Similarly, only 60% of companies which were more concerned about IT security this year than they were 12 months ago rated their approach as Proactive. At the same time, however, companies who were less concerned about IT security this year were far more likely (83%) to indicate a proactive approach to security, indicating their efforts have been paying off. The field may be maturing, but companies still have a long way to go toward establishing an IT security framework which truly minimizes organizational vulnerability.

### **ATTENTION TO IT SECURITY DRIVEN BY BUSINESS NEEDS, NOT REGULATION**

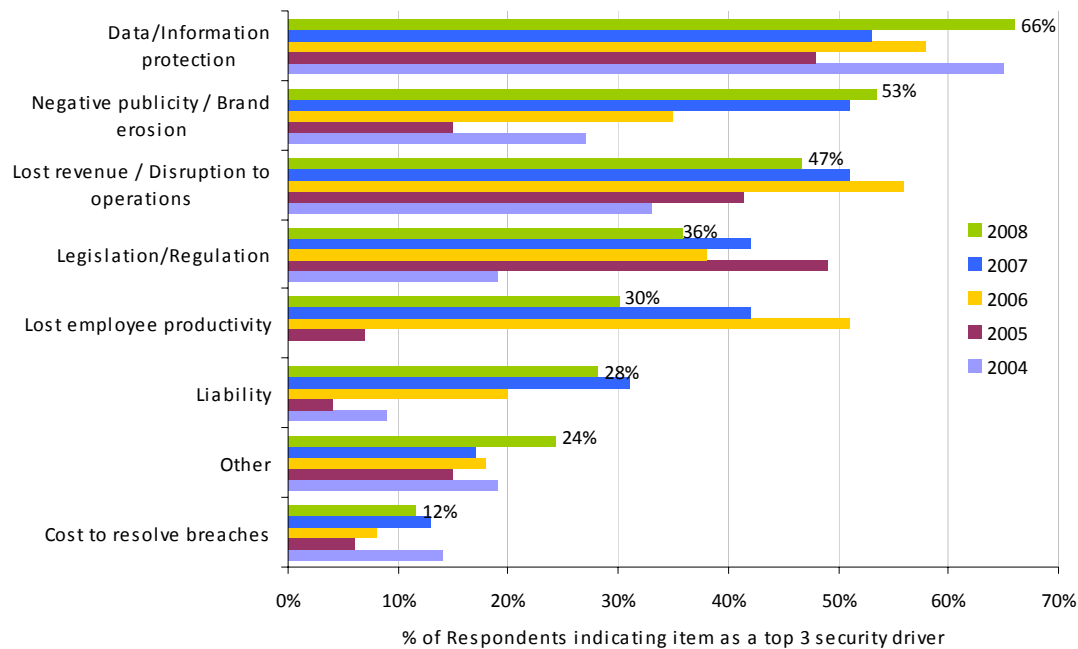
The top drivers of companies' attention to IT Security this year were data/information protection (ranked #1 by 39% of respondents), lost revenue due to disruption to business operations (ranked #1 by 19%), and the reputational risks associated with negative publicity (ranked #1 by 17%).

**Data/Information Protection** remains the perennial #1 concern of large organizations, having ranked #1 among the Top 3 security concerns each year since 2004, with the exception of 2005, when it was briefly unseated by Legislation. This year, the importance of data protection as a Top 3 security driver has increased by 13% (the most of all drivers), to 66% of respondents. Data protection was most frequently listed as the #1 concern for respondents in the Education, Energy and Insurance sectors. This category includes the protection of crucial business information, as well as the protection of client data.

**Reputational Risks** including negative publicity and brand erosion rose slightly in importance this year, as 53% of all respondents ranked it among the Top 3 security drivers. This is up significantly from 27%, when the question was first asked in 2004. Negative publicity was the #1 concern for Financial Services and Telecommunications companies.

**Lost revenue due to disruption of business operations**, while down by 4% this year and 9% since 2006, is still the third most important driver this year, with 47% of respondents ranking it among the Top 3. This represents a much greater awareness of the financial implications of IT security breaches than in 2004, when only 33% of respondents ranked it highly. The decline during the past two years is due in part to

Figure 4 - Top 3 Drivers of Security  
(2004 - 2008)



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

some companies' greater ability to limit the destructive impact of a breach through proactive monitoring and effective response procedures. However, in some cases it is a result of underestimating the true cost of a breach, which includes both direct and indirect costs, the latter of which are rarely measured.

**Legislation/Regulation** was ranked among the Top 3 drivers of security by 36% of respondents this year; however, it was only ranked #1 by 8% of organizations and its presence in the top 3 has declined by 6% this year and 13% from its all-time high of 49% in 2005, when it ranked #1 among all security drivers. While legislation is undoubtedly important, the study findings indicate that the majority of organizations are motivated more by the business imperatives of protecting their data, their finances, and their reputations.

#### ATTENTION TO IT LEGISLATION DRIVEN BY INVESTORS AND LEGAL CONCERNS

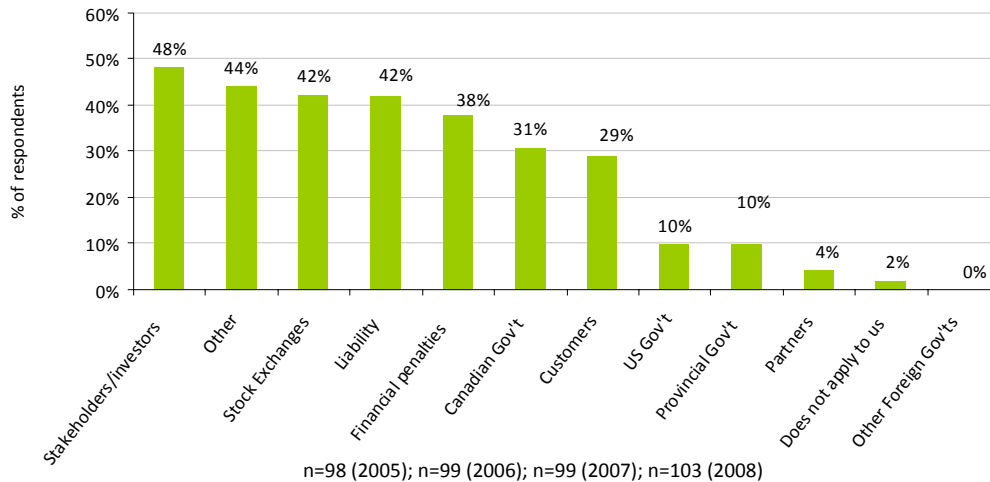
When asked to rank the top drivers behind their organizations' attention to IT security legislation, the drivers ranked #1 most frequently included

- » Stock exchanges (24%);
- » Stakeholders and investors' demands for better governance (17%); and
- » Financial penalties (10%)

The drivers which most frequently appeared among the Top 3 are

- » Stakeholders and investors' demands for better governance (48% of organizations);
- » Stock Exchanges (42%);
- » Liability (42%); and
- » Financial penalties (38%).

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



The importance of **stock exchanges** (a category which includes regulations such as the Sarbanes-Oxley Act) has risen consistently in the past several years; it is up 21% as a Top 3 legislation driver since 2005, and 11% since 2007.

Stock exchanges were the most important legislative driver for the Energy, Manufacturing, and Telecommunications industries in 2008. **Stakeholders and investors**, on the other hand, were recognized as the most important driver for the financial services and insurance industries (ranked #1 by 38% of respondents in both industries), which is to be expected given the nature of the data these companies store and the increased public scrutiny of their security practices.

Other notable changes this year include the sharp decline in the stated importance of the Canadian government (-44%), US government (-24%), customers (-15%) and partners (-15%). This may be due to the introduction of three new categories this year: financial penalties, liability, and demand for better corporate governance by stakeholders and investors. It would appear that the previously high importance of the Canadian and US governments in driving attention to IT security legislation has been largely as a result of these governments' ability to dispense financial penalties to respondents.

Additionally, the number of respondents who claimed that regulations did not generally apply to them declined to 2%, from 12% last year. It seems that companies have let go of their naïveté in regard to the legal consequences of IT security breaches.

## RISK OF ATTACK

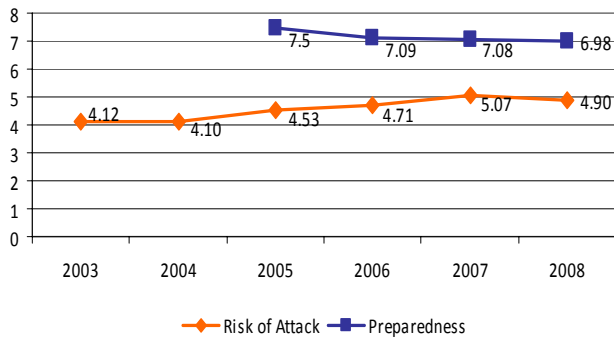
### RISK OF ATTACK RELATIVE TO PREPAREDNESS MAY BE ON THE RISE

An interesting trend has emerged during the past five years: while IT managers continue to believe that their organization's vulnerability to security breaches is moderate but increasing, they believe that their ability to deal with a security breach is on the decline. Organizations' perceived vulnerability has risen from 4.53 in 2005 to 4.9 in 2008, while preparedness has fallen from 7.5 in 2005 to 6.98 in 2008. This has meant that the spread between preparedness and vulnerability has fallen from 2.97 to 2.07 – a decline of about 30% in just three years.

This suggests, once again, that as organizations put systems in place to manage IT security, they are at risk of complacency about responding to new and ever-evolving threats in their IT environment.

The industries which indicated the highest perceived risk this year included education, insurance and retail. Those with the lowest perceived risk to an IT security breach included manufacturing, financial services and telecommunications.

Figure 6 - Risk of Security Breach vs. Preparedness



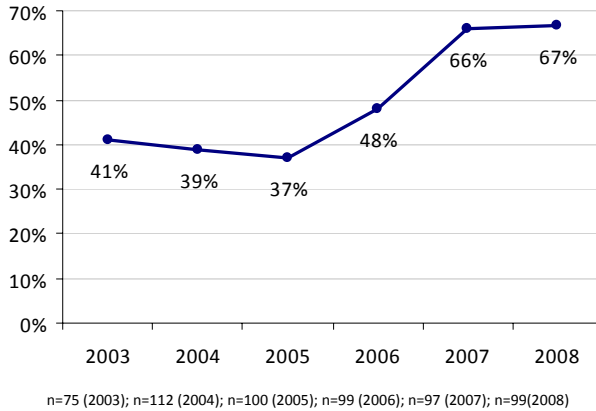
**TABLE 1**  
**RISK VS. PREPAREDNESS**

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

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

## WILLINGNESS TO DISCLOSE BREACHES STAGNATES AT TWO-THIRDS OF ORGANIZATIONS

Figure 7 - Willingness to Disclose Breaches  
(2003 - 2008)



Another significant trend that has occurred during the past three years is companies' increased willingness to disclose security breaches, which appears to have leveled off at roughly 2/3 of all companies. During the 2003-2005 period, companies were much more secretive about security breaches than they are now, perhaps because breaches were so widely publicized and companies whose vulnerabilities were exposed to the public faced much disapprobation and negative publicity. In addition, 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.

In the past three years, however, it appears that as technology for dealing with breaches has improved and the idea of security vulnerabilities has lost some of its sensationalism for the public, companies have become more willing to disclose breaches and publicize their effective resolution. This is a positive trend, which makes it less likely that customers' data will be compromised without their knowledge. However, it still leaves 33% of breaches undisclosed – a disconcerting statistic which will likely not disappear until tougher laws are enacted.

## THEFT, FRAUD AND PHISHING ARE ON THE RISE AS ATTACKS BECOME MORE SOPHISTICATED

IT Security breaches can take many forms. In 2008, the top five types of security breaches experienced by companies included SPAM, viruses, spyware, security policy violations and phishing. Attacks in general are on the rise: the average company experienced 6.7 different types of security breaches this year, up from 6.0 last year.

The highest rates of growth were in the following areas:

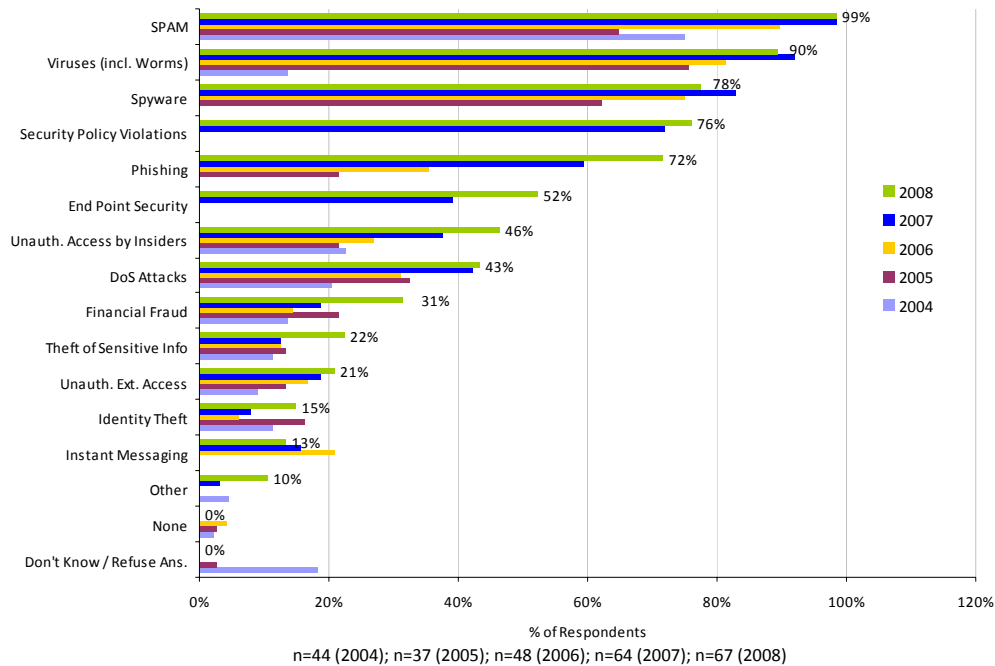
- » Identity theft (91% more companies reported this breach in 2008 than in 2007)
- » Theft of sensitive information (+79%)
- » Financial fraud (+67%)
- » End point security (+34%)
- » Unauthorized access by insiders (+23%)
- » Phishing (+21%)

Those areas that decreased slightly consisted of the following:

- » Instant Messaging (-14%)
- » Spyware (-6%)
- » Viruses (-3%)

The modest but encouraging declines in spyware and viruses may represent a greater level of preparedness on the part of companies to deal with these very common types of breaches. Moreover, it appears that hackers and fraudsters have become more sophisticated in response to better security in target organizations, and have invested more of their energy in phishing and financial fraud. The decline in reported attacks in Instant Messaging also comes as a surprise, given that many security experts report a rise in these attacks as a significant ongoing trend. However, this perceived decline may be due to the difficulty of measuring the number of breaches which may have indirectly resulted from instant

Figure 8 - Security Breaches Experienced (2004 - 2008)



messaging. It may also be due to the fact that many large corporations and most government entities have banned instant messaging altogether.

On the whole, it is clear that the number and severity of attacks are on the rise, since some of the greatest increases occurred in precisely the driver of IT security that concerns companies the most – the protection of data and information. Clearly, the rise in both the importance of data security and breaches of data security calls for greater investment and attention to this crucial domain.

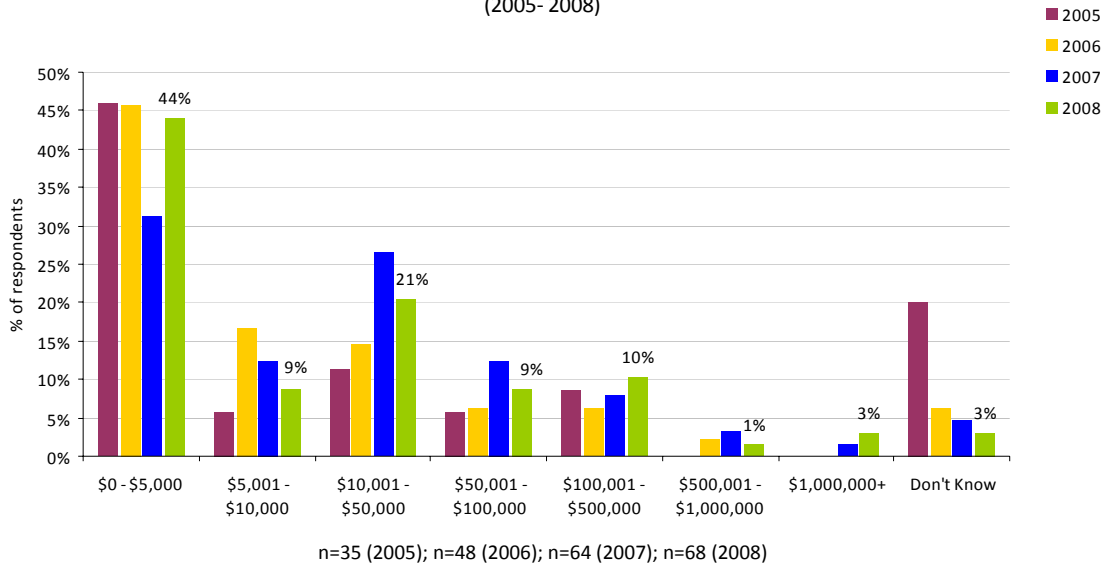
**GROWTH IN ANNUAL SPENDING ON BREACHES IS AT THE TOP AND BOTTOM OF THE COST SPECTRUM**

In terms of the total cost of breaches, three categories showed increases this year. The proportion of companies that reported spending \$0-\$5,000 to resolve breaches increased from 31% to 44% of the total. At the same time, the proportion of companies that had to spend \$500,001-\$1,000,000 increased 25% (from 8% to 10% of the total) and the number of companies in the \$1M+ category increased slightly, from 2% to 3%.

The increase in companies experiencing costly attacks indicates that the increase in financial fraud, theft and phishing, as noted above, is taking its toll on organizations. However, the increase in companies

spending less than \$5,000 on breaches, while due in part to improved security in some organizations, also seems to indicate that organizations remain unaware of the true total costs breaches pose.

Figure 9 - Estimated Total Annual Cost to Resolve Security Breaches (2005- 2008)



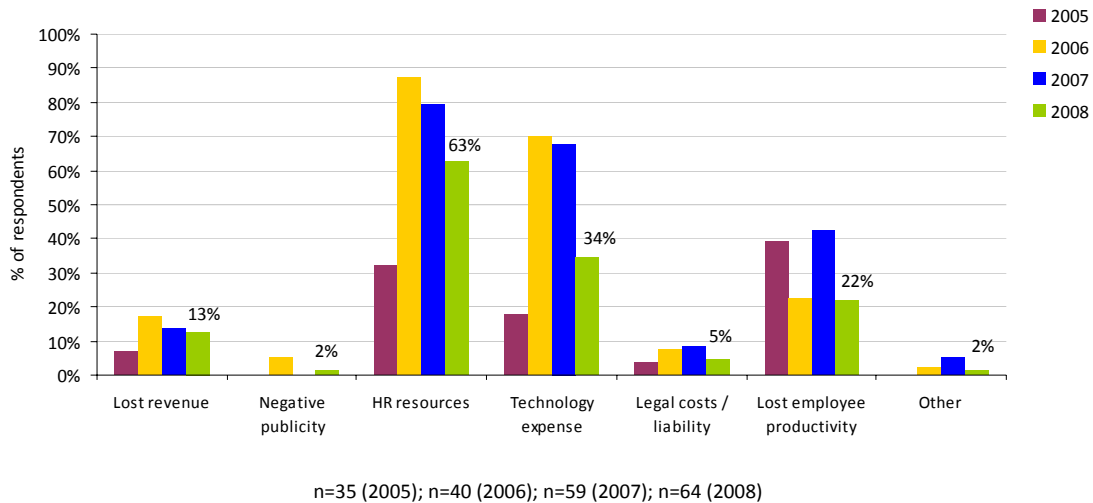
#### COMPANIES REPORTING FEWER COSTS FROM BREACHES THIS YEAR

When asked what comprised the cost their companies incurred as a result of breaches, the majority of respondents cited the same three major categories as they had in the previous two years - human resources (63% of companies), technology expense (34%), and lost employee productivity (22%). However, while the ranking of expenses remain the same, the propensity of companies to report them has declined considerably this year (with the exception of “negative publicity, which is up from 0% to 2%). The change in the proportion of companies including the following expenses in their estimates is:

- » Technology expense (-49%)
- » Lost employee productivity (-48%)
- » Legal costs/liability (-45%)
- » Human resources (-22%)
- » Lost revenue (-8%)

The fact that companies are less likely to include each of these costs in their calculations this year may be responsible in part for the rise in the percentage of companies that report spending less than \$5,000 on resolving security breaches. This does not necessarily mean that the occurrence of these costs has declined; it only shows that companies are less likely to take these costs into account when estimating the total costs of IT security breaches. Of course, it is probable that some companies have developed strong systems to stop security threats early, thus avoiding many of the expenses they incurred in the past.

Figure 10 - Primary Costs Caused by Security Breaches



Just as in past years, however, it appears that companies underestimate the true cost of security breaches, classifying important costs as overhead rather than measuring and tracking the true cost of security vulnerabilities. This dangerous practice can lead decision-makers to underestimate an organization’s true vulnerability to significant threats, and to result in a greater incidence of expensive attacks – an impact some companies are already experiencing.

### CANADA’S THREATSCAPE REFLECTS FINANCIALLY MOTIVATED ATTACKERS

Threats to IT security can take a range of 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 technique used 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 have become more varied and professional in the past two years, with Symantec’s recent Internet Security Threat reports noting a trend toward web-based attacks, end-user targeting, and a significant increase of phishing and other activities with the goal of financial gain.

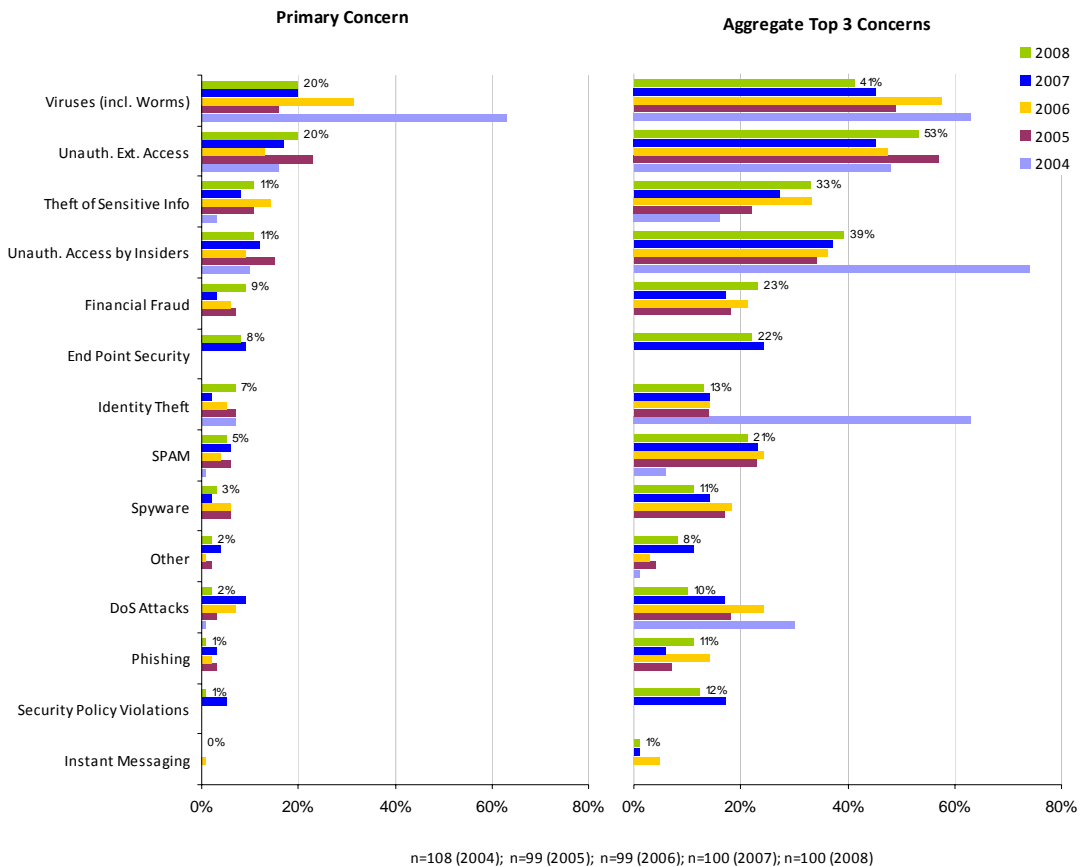
The four most significant concerns among Canadian IT executives are **viruses** (the #1 concern for 20% of respondents), **unauthorized external access** (20%), **unauthorized access by insiders** (11%) and **theft of sensitive information** (11%, up from 8% in 2007). This year, **end-point security** has dropped to #6 from #4 among top-ranked threats (as the top concern for 8%, rather than 9% of companies), despite the increasing number of infection routes and types of devices to secure. Conversely, concern about **financial fraud**, which is increasingly becoming a major motivation behind security breaches, has increased threefold since last year: 9% of companies ranked it their top concern in 2008, up from just 3% last year.

A look at the year-over-year changes in threats that companies list among their Top 3 concerns reveals that organizations are realizing the increased danger caused by the rise of financially motivated hackers. The greatest increases have occurred in the percentage of companies naming the following threats among their Top 3 IT Security concerns:

- » Phishing (+ 84%),
- » Financial fraud (+ 35%),
- » Theft of sensitive information (+ 22%), and
- » Unauthorized external access (+ 18%).

On the other hand, this year organizations are less concerned about DoS attacks (-41%), security policy violations (-29%), spyware (-22%) and viruses (-9%). These findings are consistent with other studies indicating that professional hackers have turned their attention to financially motivated breaches, rather than vanity projects such as DoS attacks.

**Figure 11 - Ranking of Threats (2004 - 2008)**



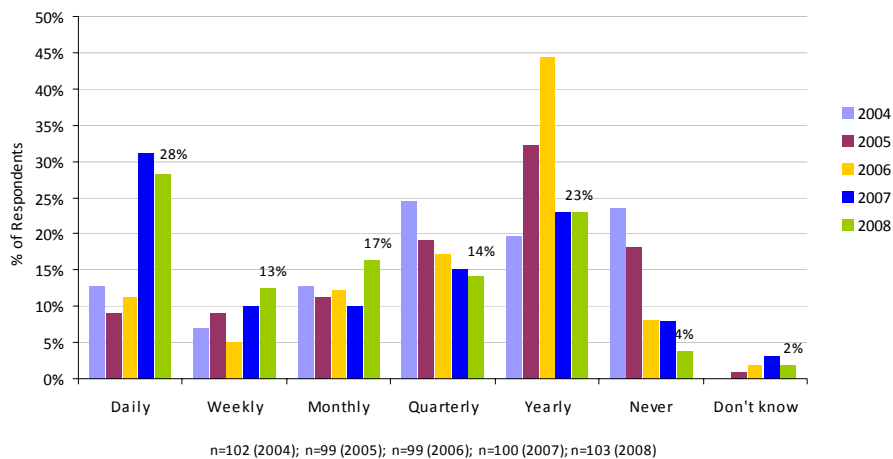
# VIRUSES

## FREQUENCY OF VIRUS ATTACKS RISES BUT DEFENSIVE TECHNOLOGY KEEPS UP

Unchanged from the past two years, viruses rank as the second most common form of attack experienced by respondents and is one of the top two concerns (ranked among the top three by 41% of organizations, second only to unauthorized external access, and representing the #1 concern for 20% of companies). While organizations are relatively less concerned about viruses this year than they were last year (largely due to the rise in frequency and importance of direct financial threats from phishing and other fraudulent activities from external intruders), viruses remain a top concern due to potential costs of remediation as well as their ability to disrupt operations and continually surprise targets with their growing diversity and sophistication.

In 2008, the proportion of respondents indicating that they experienced virus outbreaks daily has declined slightly (from 31% in 2007 to 28% in 2008), likely due to improvement in respondents' virus technologies and compliance to security policies. It is worth noting, however, that this year's 28% is still a significant increase from the 13% of respondents who reported daily outbreaks when this question was asked in 2004. On the other end of the spectrum, the proportion of organizations claiming never to have experienced a virus outbreak has also declined (from 8% to 4%), which could be due either to the increased severity of attacks on these organizations or simply their willingness to disclose the breach. Similarly, the number of companies enjoying only yearly or quarterly virus attacks has continued to decline over the past year, while the number of companies suffering from weekly or monthly outbreaks is on the rise (see Figure 12). On the whole, IT managers have had more virus headaches to deal with this year than in prior years.

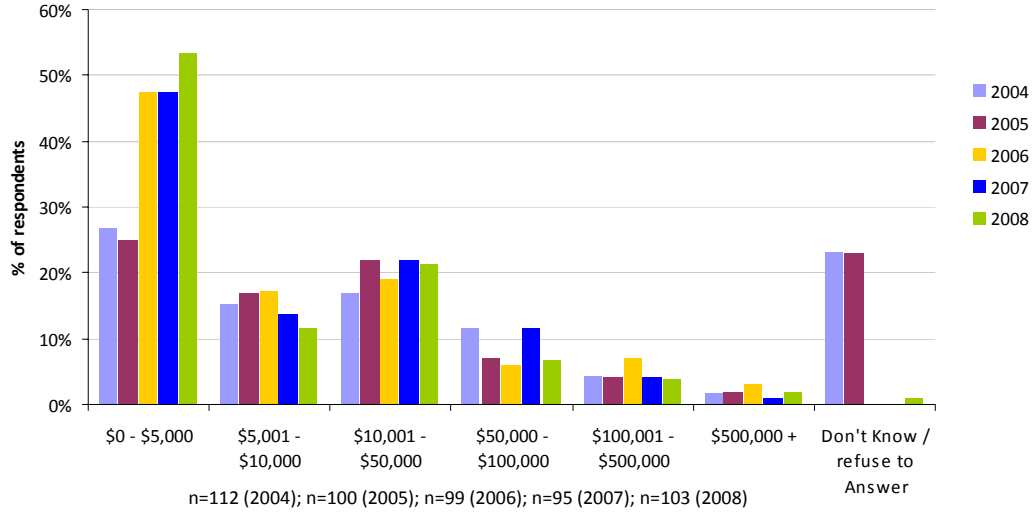
Figure 12 - Frequency of Virus Outbreaks (2004 - 2008)



Investments in virus detection and eradication tools have, however, paid off for Canadian companies in the past year: the proportion of organizations reporting an estimated cost of less than \$5,000 per virus outbreak has continued to rise to an all-time high of 53% this year, as shown in Figure 13. Conversely, the proportion of companies reporting an average cost of \$50,000-\$100,000 has fallen from 12% to 7% of the total this year while all other categories have remained relatively stable (with changes of 2% or less).

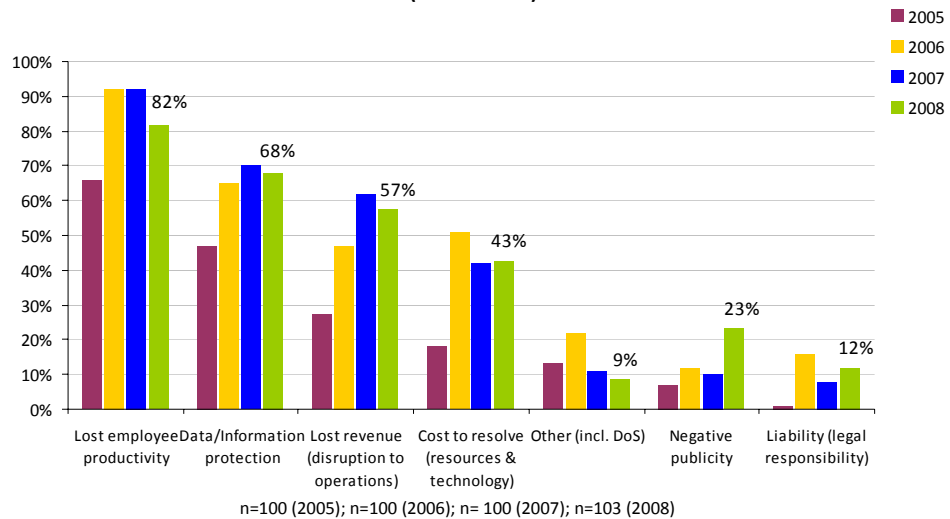
While the frequency of attacks is on the rise, it appears that defensive and preventative technologies are keeping up with hackers to minimize their impact on enterprise operations.

**Figure 13 - Cost to Resolve a Virus Outbreak**



As figure 14 shows, the perceived threats resulting from virus outbreaks are similar this year to last year, 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 for IT executives.

**Figure 14 - Ranking of Top 3 Consequences of Virus Outbreaks (2005 to 2008)**



**Lost employee productivity**, while still the top concern, has diminished in significance – this year, it is among the top 3 concerns for 82% of companies, down from 92% last year. This is likely due to the reduced perceived cost and damage from an average outbreak this year (see above).

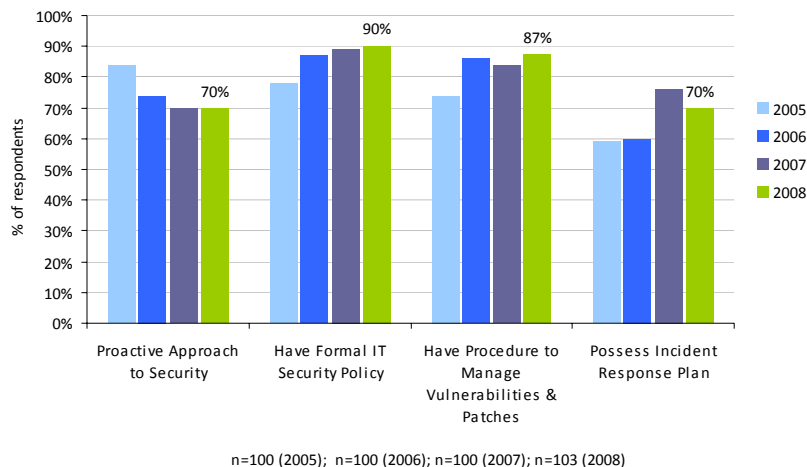
The biggest increase has occurred in the number of companies concerned about **negative publicity** as a result of virus outbreaks, which reached an all-time high of 22% this year. It can be hypothesized that this is due to some of the more disruptive viruses which have the potential to compromise customer data security – the threat that is most likely to attract media attention.

## PREPARATION, PREVENTION AND MANAGEMENT

### WHILE ADOPTION OF SECURITY MEASURES IS STRONG, GROWTH IN ADOPTION IS DISAPPOINTING

Although IT security departments are often criticized for taking a reactive, tactical, and silo-based approach to security management (indeed, some do), the majority of companies surveyed are continuing to proactively and strategically manage IT security.

Figure 15 - IT Security Policy & Processes

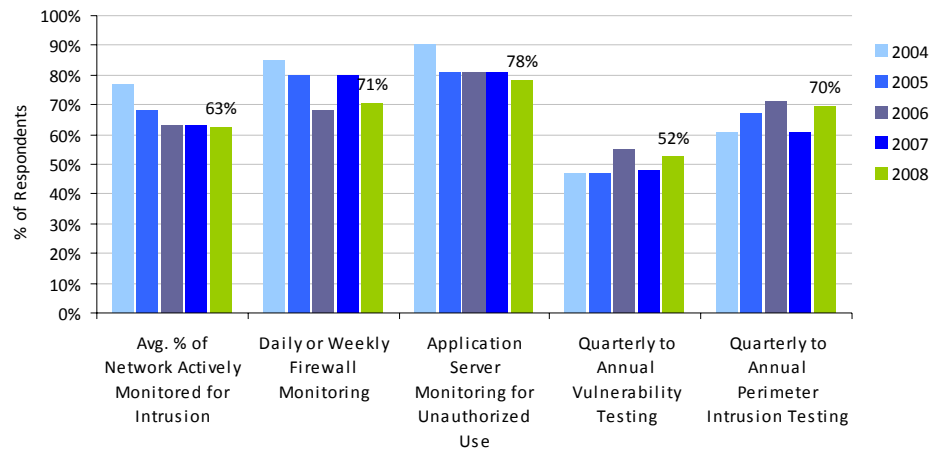


This year, the percentage of companies claiming to have a proactive approach to security is the same as it was last year (70%), down from a high of 84% in 2005. However, 90% of companies also report having a formal IT security policy in place and 87% have a procedure in place to manage vulnerabilities and patches. This represents a continued understanding that IT security is not something to be managed by IT alone, but rather requires a coordinated effort between technical, legal, and public relations management activities, particularly in the event of a significant data security breach.

While more adoption of these proactive measures would be desirable, it is nonetheless apparent that the majority of companies are making an effort to deal with the ever-growing threats they face. For companies that do rank themselves as “proactive,” this effort is paying off: 35% of proactive companies are more concerned about IT security this year, whereas 55% of companies with a reactive approach have found reasons to be more concerned.

The adoption of tactical initiatives, including network, firewall, and application server monitoring for intrusions, continues to be strong in 2008. However, all three of these categories are down slightly from last year and particularly from 2004. Adoption of proactive measures also remains strong: 83% of organizations run regular vulnerability assessment scans, while 82% run regular perimeter penetration testing.

Figure 16 - Security Processes Employed



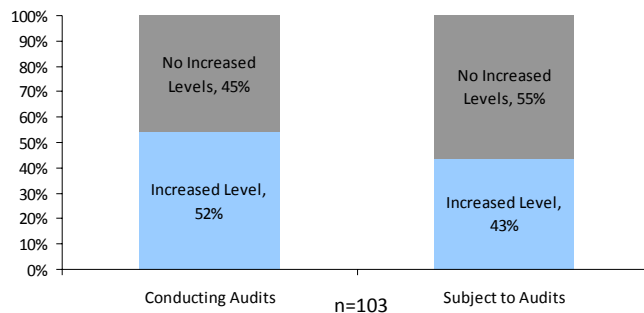
n= 93 to 112 depending on question and year

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

- » **Active intrusion monitoring** – Overall, 63% of networks are actively monitored for intrusions. The average percentage of networks monitored for intrusions in 2008 was 63% (stable from 2007, but down from 77% in 2004). Clearly, there is much room for improvement in this stagnating area.
- » **Firewall monitoring** – Firewalls are a company's first line of defense against intrusions, and their importance in protecting corporate data should not be underestimated. This year, only 71% of companies reported daily or weekly firewall monitoring (down 11% from last year), although a respectable 21% report monthly or quarterly monitoring.
- » **Application server monitoring** – This important security tool has actually declined in adoption in 2008 after three years of stagnating. Currently, 22% of Canadian companies do not monitor their application servers for intrusions, up from 19% in 2007.
- » **Vulnerability Assessments** – As many as 17% of large Canadian organizations do not run regular vulnerability assessment scans, which are a key preventative IT security tool. Among those who do perform them, only 30% do so daily, weekly or monthly, and 52% do it quarterly, semi-annually or annually.
- » **Perimeter penetration testing** – This year, 82% of companies conducted regular perimeter penetration testing. Of these, 13% did so daily, weekly or monthly, while 70% did so quarterly, semi-annually or annually. Alarming, as many as 9% of respondents indicated that they never conducted perimeter penetration testing.
- » **Incident Response Plans** - One disconcerting trend to watch next year is the reduced adoption of incident response plans among respondent companies: in 2008, 70% of companies reported having one (8.4% fewer than last year).

- » **Formal procedure to manage and implement patches** – Considering that 73% of vulnerabilities are classified as “easily exploitable,”<sup>6</sup> and that time to patch is significantly longer than time to exploit, it is crucial for IT organizations to manage this risk with a speedy patch management procedure. Indeed, 87% of organizations surveyed had one in place (up slightly from 84% in 2007).
  
- » **Partner audits:** This year, 52% of respondents reported conducting more security/privacy audits with partners. 43% reported being subjected to an increased level of audits. This rate of growth is slightly lower than last year’s, but is still significant and represents an important proactive step for large organizations that increasingly operate as part of interconnected global supply chains.

Figure 17- Security / Privacy Audit Activity (2008)



While the majority of companies have adopted these essential measures to protect themselves against security breaches, greater adoption is needed. The fact that the trend in adoption in the past four years has been rather flat is disappointing, considering that respondents are more concerned than ever about protecting their data, and cybercriminals are ensuring that they have reason to be concerned.

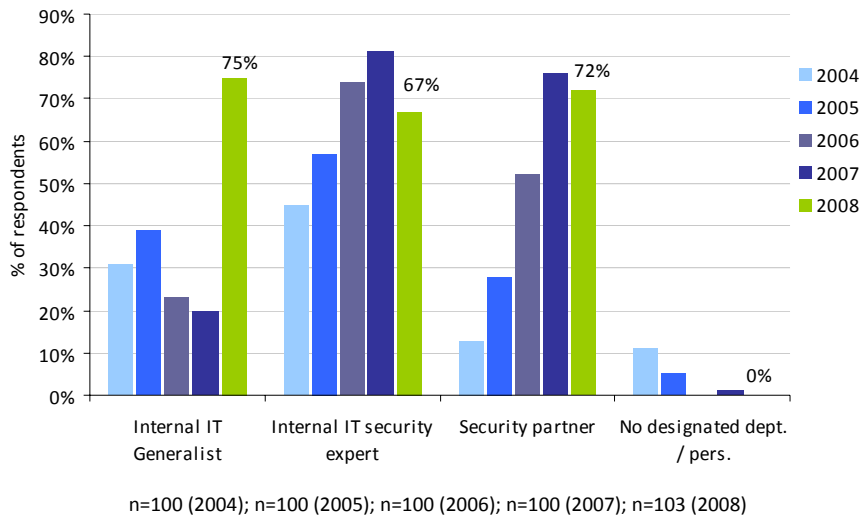
## IT SECURITY RESOURCING

Several important trends have come to bear on Canadian companies’ security HR approaches, including the increasing strategic value of IT security, the adoption of security partners for delivering some IT services, and the slowing economy. One trend in IT management among Canadian companies has been toward increasing adoption of Chief Security Officers (CSO) and Chief Privacy Officers (CPO). The reported use of both among respondents increased this year — 7% more companies (31% in total) reported having a CSO, while 6% more companies (34% in total) reported having a CPO.

In 2008, 72% of companies reported using a security partner to meet some of their security needs. While down from 76% in 2007, this nonetheless represents a very strong adoption of external IT partners. At the same time, it appears that the role of internal IT security experts has diminished slightly – perhaps in part because the increased use of security partners has worked its way through the system and allowed companies to cut back on spending on internal security experts. Conversely, 75% of companies report using an internal IT security generalist to handle at least some of their IT security, up more than three-fold from 20% in 2007.

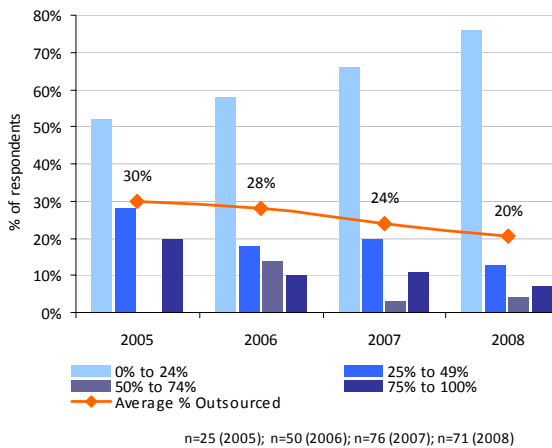
<sup>6</sup> “Symantec Internet Security Threat Report: Trends for July – December 07”. Vol. XIII, Published April 2008.

**Figure 18 - IT Security HR Approaches**

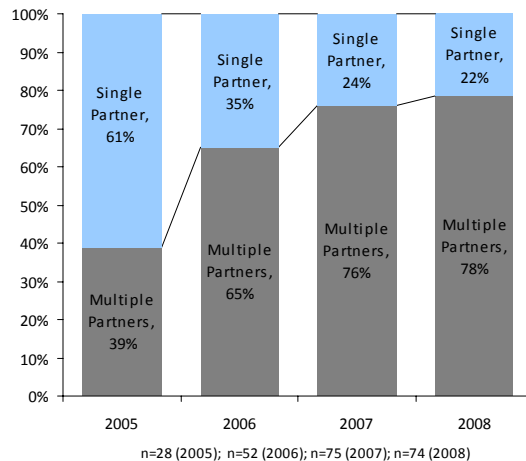


While the use of security partners has remained strong in 2008, the proportion of security they deliver has diminished each year since 2005, from a high of 30% to this year's 20%. At the same time, the use of multiple partners has once again grown to 78%. In 2008, companies again reported being quite satisfied with external partners' performance (an average of 7.31/10, down slightly from 7.69 in 2007). The trend toward using multiple partners appears to be due not to dissatisfaction with partners, but rather to specialization among vendors and companies' desire to use best-of-breed vendors for key activities and to ensure reliability through redundancy and complementary services provided by different vendors.

**Figure 19 - Outsourcing Practices**  
% of Security Delivered by Business Partners



**Figure 20 - Outsourcing Practices**  
Multiple Partner Use

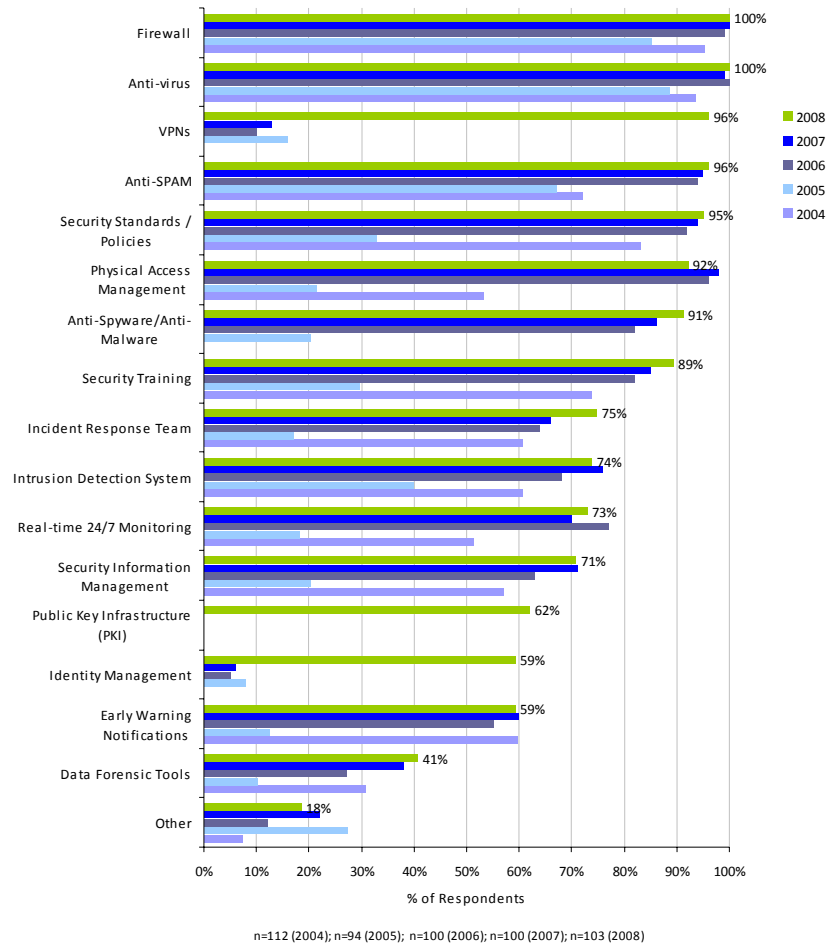


## CURRENT PREVENTION MEASURES AND INVESTMENT

Reflecting the maturity of organizations' IT security investments, most of the foundational security measures have been adopted by the vast majority of large enterprises. As figure 21 shows, virus and firewall protection software has been adopted by 100% of respondents, followed closely by anti-SPAM software and VPNs at 96%.<sup>7</sup> Areas of growth in 2008 have included incident response teams, data forensic tools, anti-spyware and anti-malware software, as well as security training.

This year's survey included three new categories: public key infrastructure (or PKI), identity management, and VPNs (virtual private networks), which have been adopted by 62%, 59% and 96% of respondents, respectively.<sup>8</sup>

Figure 21 - IT Security Inventory



<sup>7</sup> Please note that this is the first year that respondents were asked about identity management and VPNs as a separate category; the year-over-year growth rates are inflated as a result.

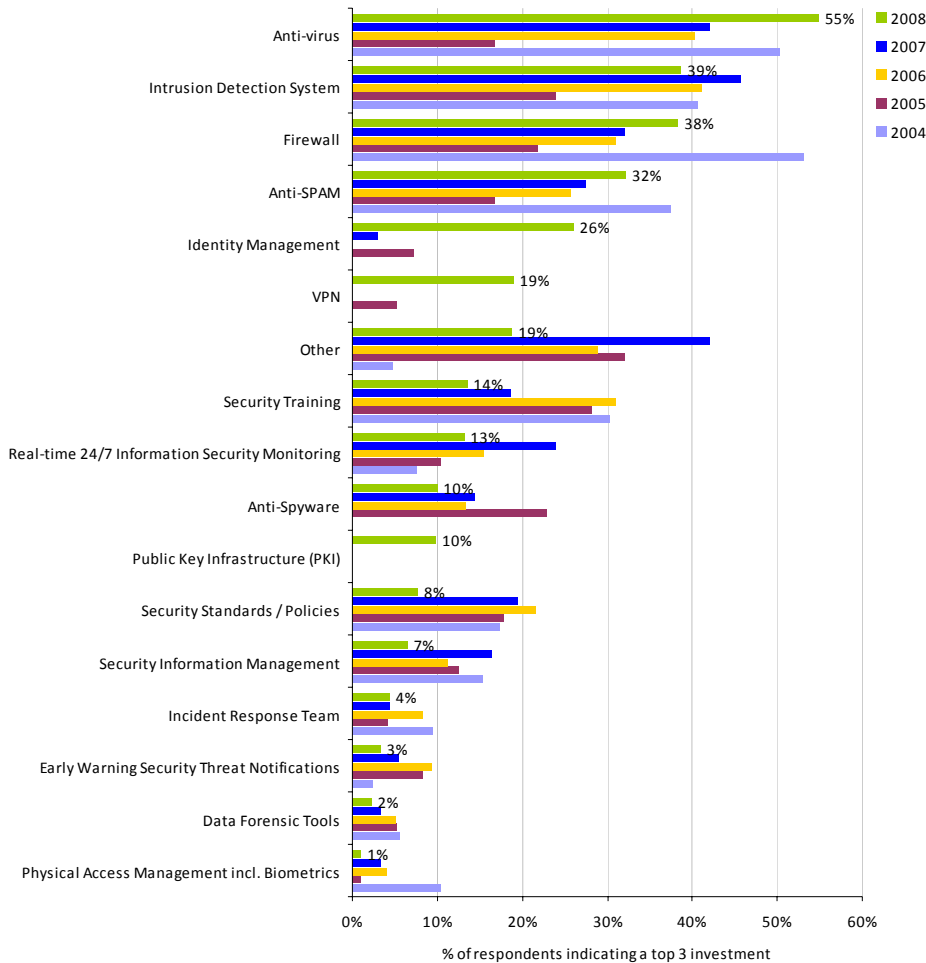
<sup>8</sup> Please note that this is the first year that respondents were asked about identity management and VPNs as a separate category; the year-over-year growth rates are inflated as a result.

Only one category – physical access management – experienced a reported decline in adoption. In general, the adoption of tools and technologies has continued to grow, both for tactical tools such as incident response teams (up 13% from last year) and proactive measures such as security training (up 5%).

**SPENDING PLANS ARE DOWN IN MOST AREAS OF IT SECURITY**

This year’s spending plans are far more modest than last year’s in many areas of security, likely due in part to an already mature security arsenal and in part to more conservative budgeting in a slowing economic environment. For example, this year, 60% fewer companies reported plans to invest in security information management; 61% fewer companies plan to invest in security standards/policies, 39% fewer companies plan to invest in biometrics; 45% fewer companies plan to invest in real-time 24/7 information security monitoring and 27% fewer companies plan to invest in security training.

Figure 22 - IT Security Investment Plans (2004 -2008)



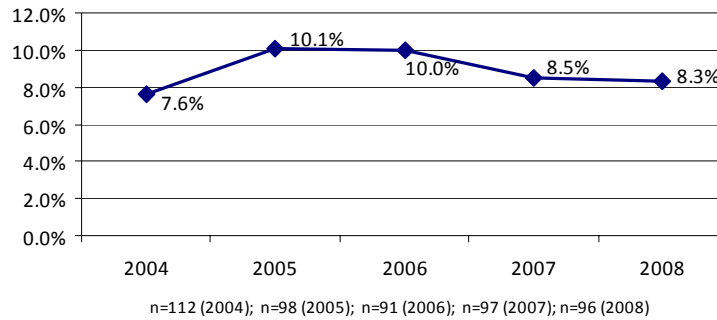
n=101 (2004); n=96 (2005); n=96 (2006); n=95 (2007); n=93 (2008)

However, investment plans are up 30% for virus protection, 20% for firewalls, and 17% for anti-SPAM software, reflecting the importance of these basic measures to corporate security and the significant return on investment they can generate.

## IT SECURITY SPENDING TRENDS AND PLANS

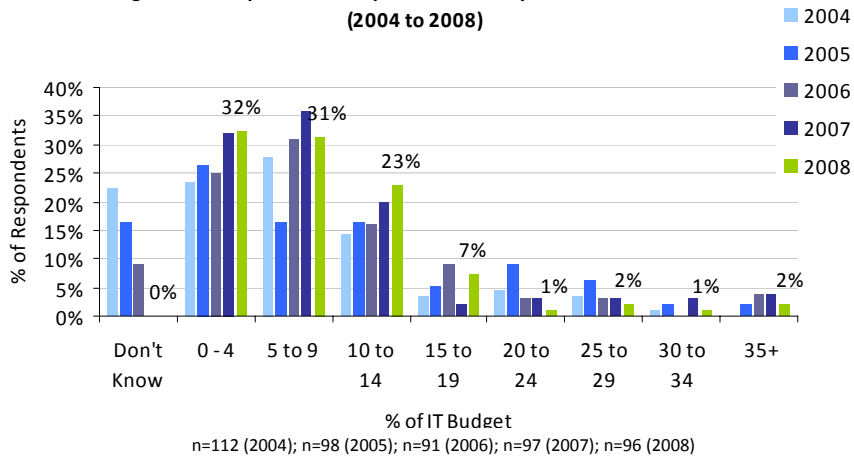
In 2008, the proportion of total IT spending for Canadian companies on IT security has declined slightly, from 8.5% to 8.3%, representing a continued decline from a high of 10.1% in 2005. Median spending remains firmly at 5%, where it has been in 2004, 2006 and 2007 (briefly increasing to 6% in 2005).

**Figure 23 - IT Security Spend as a % of Total IT Spending**



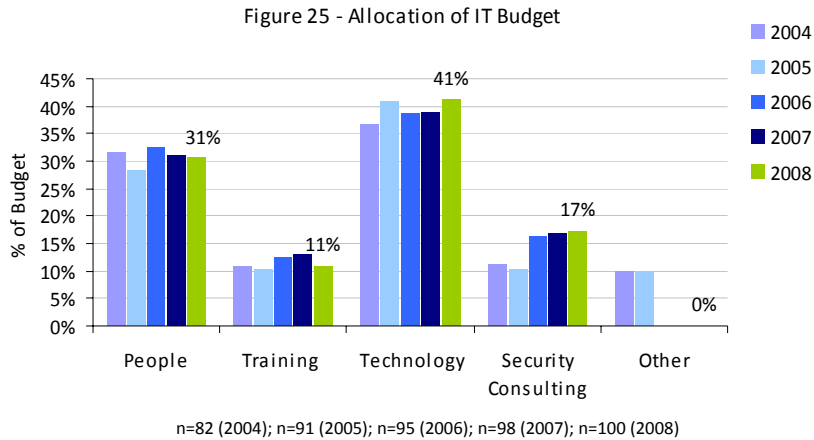
Encouragingly, while the proportion of companies spending less than 4% on security is still greater than any other (stable this year at 32%), the proportion of companies spending 10-14% rose from 20% to 23% while companies in the 15-19% categories rose from 2% to 7%. The financial services, manufacturing, and

**Figure 24 - Proportion of IT Spend on Security Products & Services (2004 to 2008)**



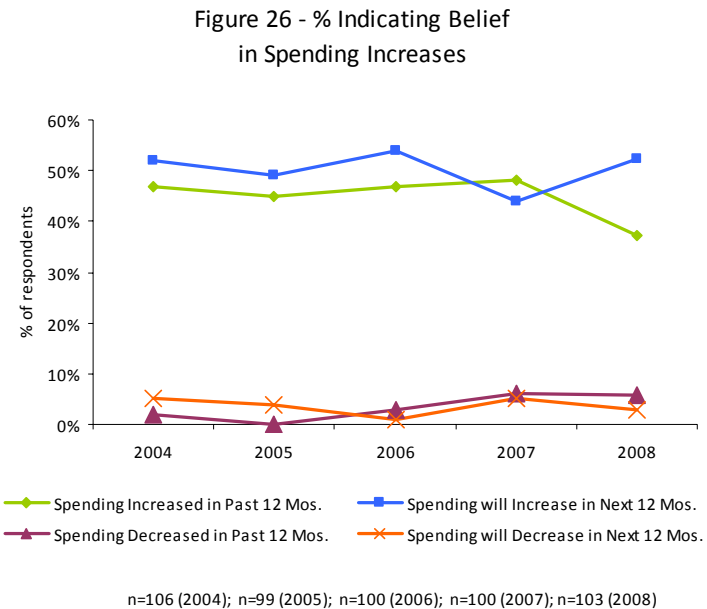
telecommunications sectors reported that some of the greatest proportions of their budgets were spent on security. On the other hand, the energy, natural resources and retail sectors lagged behind the average.

As Figure 25 shows, technology costs continue to account for the great portion (41%) of Canadian companies' IT investments. The relative importance of both technology and security consulting as a portion of the budget has grown since 2004. Spending on people has remained stable at 31%, while the relative decline in spending on training (from 13% to 11% of the overall budget) is disconcerting, as the reported number of security policy violations has also increased this year.



IT security managers' perception of security spending has dropped in the past year – 37% believe that spending increased in the past 12 months (lower than the already-cautious 44% who had predicted an increase 12 months ago). In general, the predictions of increased spending are slightly on the optimistic side, with a lower proportion of respondents indicating an increase in spending the following year.

However, 2007 marked an additional decrease in spending expectations, with the percentage expecting increased spending down to 44% from 54% in 2006). In addition, the percentage of IT managers reporting an increase in spending in the past year dropped to an all-time low of 37% in 2008, down from 48% last year. This is likely due to both spending caution in a slowing economy and the confidence many companies have in their existing systems. This year, IT managers' spending expectations are once again on the rise, with 52% expecting a spending increase. This is likely due to a need to catch up on key investment areas after a drop in spending last year.



## CONCLUSION

---

With the growing sophistication of attackers, Canadian enterprises have reported experiencing a greater number of security breaches this year than ever before. Many of these threats were aimed at data theft and fraud, resulting in significant growth in IT executives' concern about data and information protection, which was already their #1 priority.

In 2008, attacks on IT infrastructures are coming from more fronts than ever before. Web applications, which are increasingly used by businesses yet reveal shocking levels of vulnerability, are becoming an important new front in the war for data security. In addition, the use of portable devices, instant messaging, and web 2.0 technologies for activities spanning home and work are opening large organizations up to attacks in ways they could not have predicted in 2003, when this study first began.

During the past five years, many encouraging trends have been documented in how Canadian enterprises' approach IT security. Canadian companies have adopted essential technologies, become more proactive in using organizational controls in addition to technological solutions, and have begun to approach security in a much more strategic manner.

However, in the past year, IT spending and planned IT investments have shown a disconcerting downward trend, as has the percentage of companies listing security as a Top 5 priority. This has occurred in spite of the fact that many IT executives believe that they are less prepared to deal with new threats now than they were in previous years. As the industry has matured and organizations have invested significant funds into deploying new technologies, it is easy to become complacent. However, the great variety of threats in the environment requires that companies stay vigilant. IT security affects the company in many important ways, and the consequences of a breach can be damaging to an entire corporation, not simply to its IT department. To respond to new threats, increasing the use of proactive practices and continued spending are more important now than they have ever been.