

Symantec 2007

Pulse of IT Security in Canada

Volume V

The annual Symantec Pulse of IT Security in Canada survey, now in its fifth 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 2007.

KEY FINDINGS

Importance of IT Security

- While all respondents articulate that security is important 82% (vs. 92% last year) see it as a top 5 priority.
- Continuing its decline, the proportion of IT Security Managers more concerned with IT security compared to 12 months ago shrank to 34%, the lowest proportion ever. However, only 4% are less concerned, indicating a certain level of stabilization.
- Data protection and unauthorized access remain the top concerns due to the potential financial and legal ramifications of security breaches and data loss. Negative publicity has grown to the second most important driver of IT security management, a 70% increase from 2006.
- Slightly less than 1 in 3 companies have created positions of Chief Privacy Officer and Chief Security Officer.

Coping with a diverse threatscape

- The perceived risk of attack continues to grow, but companies appear moderately confident in their ability to respond, although no more confident than last year.
- 66% of respondents claim to be willing to admit a security breach publicly, a 38% increase from 2006.
- Reported security attacks comprise SPAM (98%), Viruses / Worms (92%), Spyware (83%) and Security Policy Violations (72%).
- The annual cost of managing security breaches continues to increase and is driven by HR costs, technology costs and lost employee productivity.

Virus/Worm Infections

- Increasing virus sophistication results in viruses remaining atop the list of primary IT security threats.
- The frequency of virus outbreaks continues to increase with 31% reporting them as daily occurrences.
- 47% of respondents estimate the cost to resolve a virus outbreak at less than \$5,000.
- IT security managers perceive lost employee productivity (92%), compromised data/information protection (70%), lost revenue (62%) and costs to resolve outbreaks (42%) as the greatest threats from virus outbreaks.

Approach to IT Security

- While most appear to be moving toward strategic IT security management approaches, tactical initiatives continue to dominate.
- Specialization is the name of game in IT security with 80% employing specialists versus 20% employing generalists.
- 76% of respondents outsource some elements of their IT security. The overall average portion of IT security outsourced has declined steadily to 24% this year from 30% in 2005.
- Continued growth in the use of multiple partners is noted with 76% employing multiple partners, up from 65% last year.

Investment in IT Security

- Among the top 3 investment plans for 2007-08 intrusion detection (46%), anti-virus (42%) and firewall investments (32%) rank highest.
- Median spending remains static at 5% of total IT budgets. 68% 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 "*Dynamic*" captured the spirit for the Canadian IT security market in 2006, then **FOCUS** embodies this year's market. While the IT security landscape remains ever changing, trends indicate that focus and resolve characterize the perspective of all participants, both IT security professionals and hackers. Specifically, the criminal elements of hacking have refined and organized themselves to an unprecedented level to focus on financial gain; whether from data theft, stolen information remarketing or malicious business disruption. This escalating organization and coordination of security breaches symbolizes the mainstreaming of cyber crime around the globe to exploit inherently fragile and vulnerable corporate IT infrastructures.

However, IT security professionals are responding to this ever-increasing and evolving array of threats that range from internal security breaches by employees to the continued proliferation of polymorphic malware delivered through bot networks of increasing scale. As a continuation of last year's strategic transformation of information technology, some corporations continue to shift their focus from tactical/reactive tools implementation to enterprise-wide strategy & process driven practices complemented by leading edge tools and applications. Although, the study results do provide evidence that suggest entrenched tactical thinking continues to impede this overall progress.

With the highly visible media reporting of confidential data breaches and increasing lawmaker scrutiny, companies possess no choice but to make concerted efforts to protect their data for fear of the public relations and legal nightmares that might ensue from a public disclosure of a data loss. This position represents a tacit recognition of the strategic importance of data, not only to business continuity, but as a key driver of competitive advantage, financial performance and shareholder value. For example, the recently publicized the data theft of over 45.7 million individuals from TJX Companies, Inc. over a 2 year period has resulted in lawsuits which, since their filing, coincide with a 5% drop on the company's stock price.

Canada is not immune to the evolving dynamics of the IT security threatscape and this year's survey shows where we stack up relative to past years. Despite our highly wired economy, we rank relatively low compared to other countries with respect to spam hosting (23), malicious codes activity (5), and bot infections (10) based on the most recent "*Symantec Internet Security Threat Report – Trends for July – December 2006*". However, in the interconnected world of the internet, geography offers no protection to threats that emanate from the world leaders in propagating malicious activity; our largest trading partner, the United States (31% of the worldwide total) and other key trading partners China (10%) and EU countries (17%).

Given the increasing importance of global trade to the Canadian economy, our ability to continue to secure data represents a key enabler of Canadian companies' integration into global value chains. Moreover, given the critical nature of Canada-US trade, with in excess of 80% of Canadian exports being shipped there and Canada representing the largest US import market, our policies and

strategies must be closely aligned to ensure the continued integrity of trade. However, discernible differences between the two countries, that pose risks to this trade, exist.

While many US states have enacted strong privacy and security legislation, and the US appears to be marching toward a stringent, federal law on data protection and breach notification, we lag significantly in Canada. This makes Canada an increasingly attractive place in which to conduct or to target cyber criminal activities. Failure to reassess this increasing gap in legislative environment could create issues in the future. Secondly, as noted last year, the propensity for Canadian companies to be smaller than other global competition continued to create a risk of under investment in data security. The challenge of proper allocation of dollars to ensure integrated responses to the growing plethora of threats only compounds this gap. This year's data substantiates this concern as it appears that Canadian IT security spending has not kept pace with other countries. As a result, we find that the data indicates that some Canadian companies have stalled in their efforts to achieve best practice levels of integrated policies, tools and processes and have reverted to treating IT security as a cost centre not an investment centre. This situation produces a potential trade disintermediation risk, as Canadian companies could become the weak link in global value chains, thereby generating in a disincentive for foreign companies to integrate themselves with Canadian firms.

As the business landscape changes to emphasize the importance of global supply chains in achieving competitive and efficient operations, the impetus to streamline and accelerate trade efficiency drives an inexorable march toward the convergence of financial, physical and information value chains in a technology platform enabled environment. Data management and security lie at the core of successful global trade. This optimized environment leverages Software as a Service (SaaS) and Service Oriented Architectures (SOA) to deliver true inter-company integration to all participants in the supply chain. However, it also creates unparalleled data security risks as companies build competitive advantage in supply chain clusters through the real-time sharing of sensitive business data. While achieving this level of integration poses a challenge for even the most technology savvy organization, the potential security risks arising from such intensive inter-company collaboration could prove catastrophic for not only a company, but for entire supply chain clusters. As such, while companies continue to invest in data process security, they have only just moved from the tactical to the strategic within their own organization. However, the game is changing yet again and now they face the task of securing their own organization, as well as collaborating with supply chain partners to secure entire supply chain networks against progressively more innovative and well-funded attackers.

The increasingly complex needs of globalization drive an unrelentingly active IT security landscape. Continued corporate value creation, in the face of threats that seek only to erode such value for criminal profit, requires focused and integrated strategic approaches and execution. The following pages highlight the state of the Canadian market and emerging issues for the Canadian IT Security Manager in the face of this challenging environment.

Introduction

This fifth annual Symantec *Pulse of IT Security in Canada* survey was conducted in March and April 2007. One hundred (100) senior managers with enterprise security responsibility were interviewed by telephone. Focusing on developing a comprehensive understanding of Information Technology ("IT") security management issues for Canadian large companies and to expose trends in the Canadian market the following themes were explored¹:

- the relative importance and drivers of security to the organization;
- the impact of legislative and customers' priority on data security and privacy trends affecting organizations;
- the relative risk of security breaches and the types of breaches being experienced;
- inventories of IT security processes and tools, as well as, key investment areas;
- security management approaches and investment areas; and
- the economics of IT security, budgets and future spending perception.

SURVEY PARAMETERS

Targets:

Canadian enterprises
Revenues > \$50 million

Respondents:

Senior IT Managers responsible for enterprise security

Respondent Type:

VP IT/IS, Security Managers,
Director/General Manager Security, IT
Security Architects, etc.

Timeframe: April - May 2007

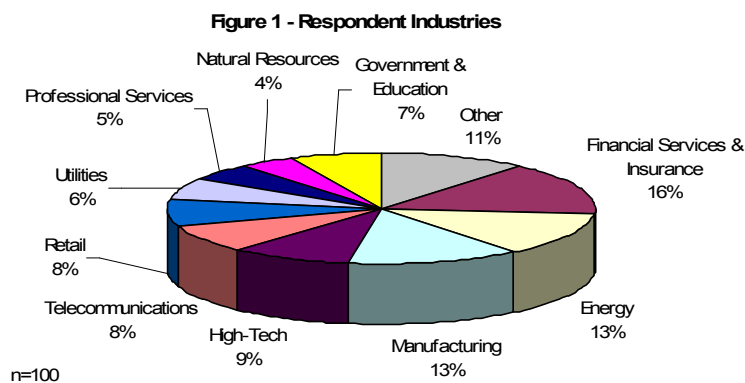
Total Respondents: 100

This report summarizes the key findings from this survey, while characterizing the evolution in the market by comparing this year's responses against those from 2003 to 2007, where relevant. Additionally, this year's study will highlight some of the vertical market responses to add a slightly different flavour to the data. While not statistically valid, these results provide additional perspective to the global data².

Respondents

As with previous surveys, this fifth instalment of the research initiative targeted Canadian companies with annual revenues in excess of \$50 million.

A diverse group of respondents comprises this year's survey base (Figure 1), led by the drivers of the Canadian economy. Financial Services and Insurance, Energy and Manufacturing are the top 3



¹ The surveys in 2005, 2006 and 2007 all contain the same questions, but differ from 2003 and 2004 in some elements, precluding comparison on these elements. Additionally several new question have been added for 2007 and are highlighted herein.

² With 100 respondents for the total survey, we cannot draw any statistically conclusions from the sector data, but only point to interesting directional findings in the various industry sectors.

participating sectors in this year's study, with a slightly more diverse group than in past years with increased participation from the High-Technology, Telecommunications and Retail segments. Given the increasing importance of these segments to IT policy in Canada the profile continues to evolve to capture the key market segments.

The Importance of Enterprise Security

Rarely does a week go by without at least one major headline referring to a recent loss of a hard drive containing employee or customer data, a breach of a credit card database, or proposed legislation to deal with the protection of confidential data. Against this backdrop, one would expect continued heightening in the importance of IT security for all IT security managers. However, 2007's data marks a 10% reduction in those reporting IT security as a top 5 corporate initiative (see Figure 2). Given the increasing sophistication of criminal intents from both external and internal threats, this

decline may signify an alarming change of direction that will require ongoing monitoring. The result could exist for any number of reasons, from an implication that security managers resign themselves to being always behind the threatscape, and therefore somewhat powerless to act, to confidence that their investments in strategies and security infrastructure offer a sound security environment, and are moving into "maintenance" mode. However, it may be also symbolic of an acknowledgement that

Figure 2 - % Indicating Security as a Top 5 Priority (2003 - 2007)

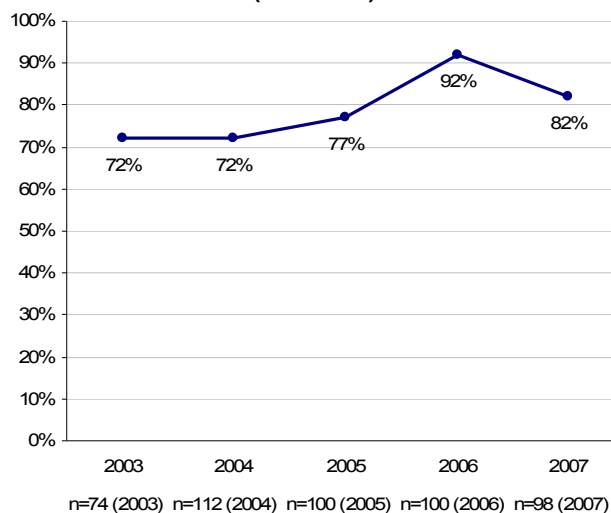
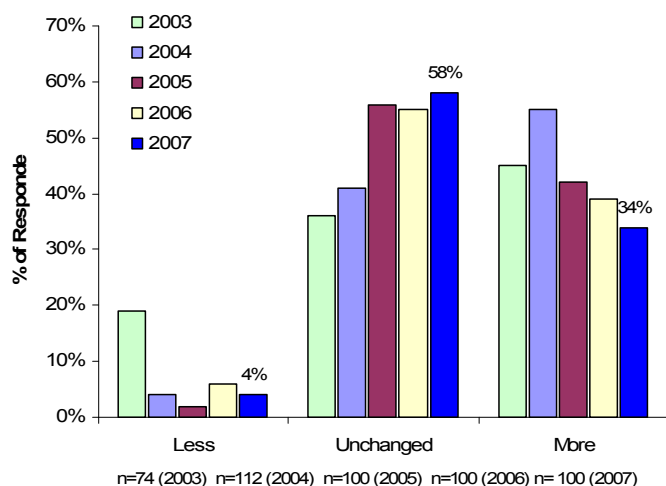


Figure 3 - Level of Concern about IT security compared to 12 months ago



IT security comprises a mainstream operating activity as opposed to a "key spending priority" like a capital project and therefore is not top of mind as a key spending priority.

In conjunction with this change in priority, the levels of concern with security continue to stabilize. 34% of respondents indicate that their security concerns have increased over the past year, the lowest in five years. However, this does not imply a diminished level of threat. With only 4% indicating a decline in their level of concern

and 58% articulating a similar level of concern to last year, the highest in five years, managers remain highly sensitive to the diversity of risks they face. Nonetheless, with the continued emergence of bot networks, polymorphic threats and proliferation of possible breaches at endpoints (USB flash memory, MP3 players, increasing use of laptops, mobile email, etc.) the steady decline from 55% being more concerned in 2004 appears to substantiate the fact companies possess an increasing level of comfort in people, practices, processes and technologies available to secure corporate data. With the continued losses of confidential data, one must question whether corporates are lulling themselves into a false sense of security.

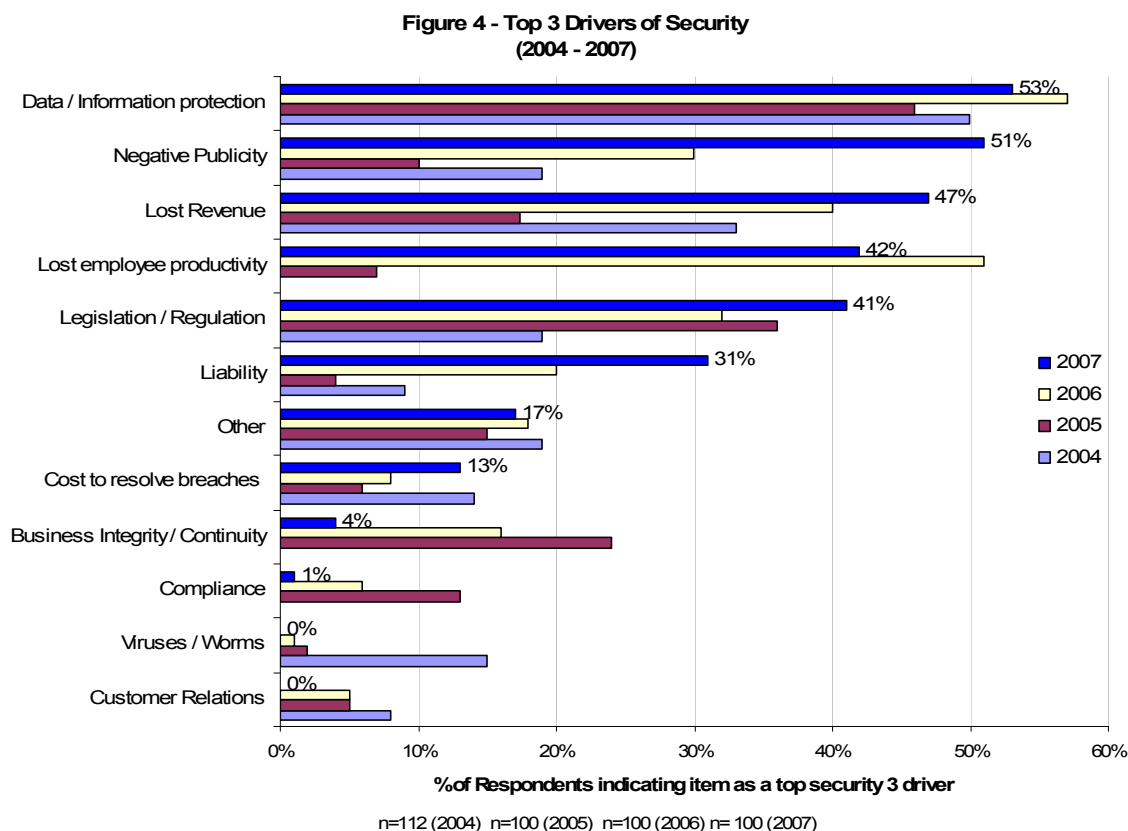
Security Drivers

Security drivers continue to consolidate around key themes:

- Data / information protection;
- Financial impacts of security breaches; and
- Liability.

These themes correspond to an interrelated set of issues and heavily influence companies' abilities to sustain their operations in a competitive market place. Moreover, 2007 exhibits a continued consolidation of drivers to focus on business performance and risk as opposed to technological issues such as malware, worms and viruses. As such, in a data-driven economy, IT security represents a critical business function which possesses the ability to heavily influence corporate performance and shareholder value.

Given such circumstances, one should think that **business continuity** would represent a key concern for respondents; however, only 4% of respondents indicated it as a primary driver of security – a continuation of the decline from a high of 24% in 2005. However, this decline may be explained by continued investment in processes and plans to deal with security breaches to minimize disruptions and the fact that lost productivity and revenue, in their own form, characterize much more specific and measurable continuity issues.



Data / information protection (a top three priority for 53%) remains the top driver and most frequently ranks as the # 1 priority for all respondents. However, its importance has declined by 7% as other issues become gradually more important. Moreover, this may be an indication of a better understanding of the technical aspects of data security, while the economic consequences of failing to do so develop into the critical reasons for pursuing security. As such, the priority to protect data exists clearly to ensure that none of the potential negative legal, business or financial ramifications ensue.

As noted previously, the increasing frequency of disclosure due to legislative requirements and liability concerns result in deeper media scrutiny of security related incidents resulting in **negative publicity** for companies involved. This driver of concern grew significantly in 2007 to the second most important issue, rising 70% (the most of any driver) from 30% in 2006 to 51% in 2007. Interestingly, this represents the most important driver for Financial Services companies indicating the importance of public confidence in their systems to sustaining their businesses, especially given the relative homogeneity of services available in the Canadian market place.

Negative publicity appears to tie closely to potential revenue impacts from disclosure of breaches. 47% (an increase of 18% from 2006) report **lost revenue** as a key driver of their security initiatives – making it the third most important security driver. The potential for customers taking their

business elsewhere represents a clear rationale for investing in security. Clearly, the damage to brand value and customer image comprises a critical consequence to a security breach that impairs the goodwill and market value of a company. As such, investment decisions appear to be driven to mitigate the potential impact on shareholder value resulting from publicized breaches of security. Other direct costs such as **lost employee productivity** (cited by 42% as a top 3 driver – down from 51% in 2006), **direct resolution costs** (13% - up from 8% in 2006) remain direct costs that continue to drive security plans.

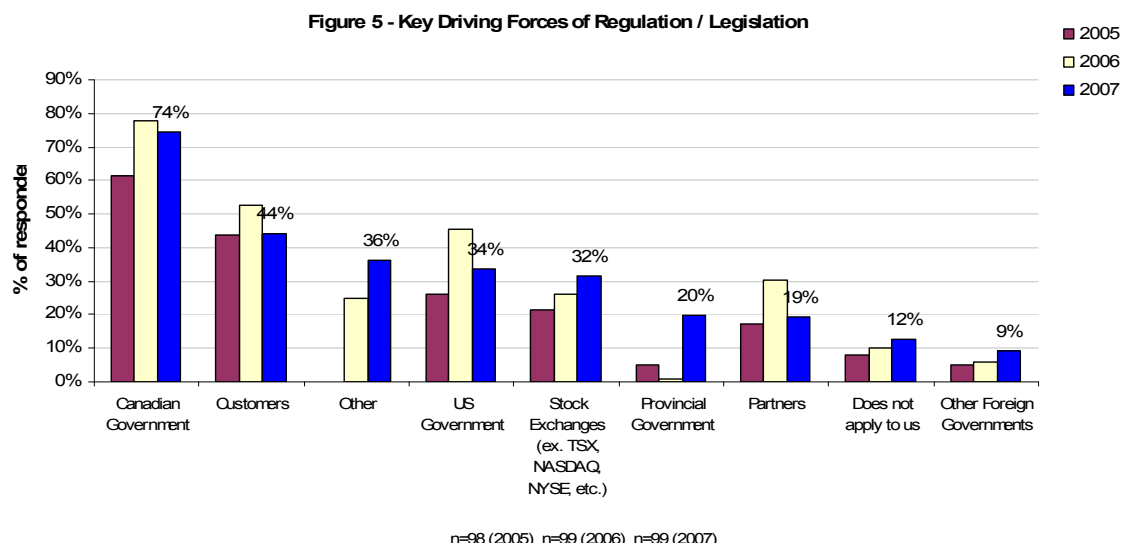
Additionally, the financial consequences not only include the potential impacts on revenue streams and shareholder value, but the potentially crippling legal costs and judgements that might arise from liability suits. This year we see a significant rise in the concerns about **liability** which increased 55% (the second most of any significant driver) to a top three issue for 31% of respondents. This represents a clear acknowledgement that companies are increasingly defending against failing to secure data appropriately. Lawsuits like those recently filed against TJX Companies, Inc. comprise the potential outcome for a failure to adequately secure such confidential data³. While the claims remain unproven, significant legal costs will be incurred to defend against such liability suits for TJX and others like ChoicePoint, Talvest and other various government agencies that have compromised client and employee data.

While the ability to prosecute such cases remains unclear due to generally weak laws and limited precedents, the sheer number of compromised data records continues to garner policy and law makers attention. Such interventions persist in propelling IT security initiatives with 41% (34% in 2006) reporting **regulation / legislation** among their top 3 drivers for security investments. A notable by-product of this amplified emphasis on regulation and legislation lies in the need to maintain ever increasing quantities of data in readily accessible, networked (or near-network), environments for easy access by auditors and regulators. This further compounds the challenges faced by IT security managers by increasing the sheer number of potential breach points into highly sensitive data.

As noted in Figure 5, the **federal government**, empowered through legislation like PIPEDA and the actions of the Privacy Commissioner of Canada, remains the most dominant source of influence on security legislation and regulation in Canada. 74% of respondents cite it as a top 3 driving force for attention to security from a legislative perspective. Moreover, increasing Canadian law maker interest for laws dealing with disclosure like those enacted by nearly 40 US states makes this driver an interesting one to watch. The possibility of a national law (which has some traction in the US) seems more distant in Canada at this time, but potential provincial privacy legislation may account for the dramatic swell in those citing provincial governments as a legislation driver (growing to 20% in 2007 from only 1% in 2006). While federal government law making ties with **stock exchanges** as

³ *Banks file suit against TJX over breach costs* SC Magazine April 25, 2007.

the driver most frequently cited as the top priority for companies having to follow security legislation developments, only 16% actually report it as the most critical driver of attention. The relative fragmentation among the cited #1 driver of attention may point towards a relatively differing set of priorities for public versus privately owned organizations and the relative risks created by different business models and customer profiles.



Respondents state **customers** to be the second most significant driver of their attention to legislation and regulation, presumably tied back to issues of data security, liability and customer confidence and increasing consumer concern over privacy of personal data. Interestingly, this year we see declines in most categories, with the exception of **provincial governments** (20%) and **stock exchanges** (32%, up from 26% in 2006) which respondents mention as their most critical drivers of attention to legislation almost as frequently they cite federal government activities as their most critical driver. These could be tied to potential changes in provincial privacy and liability laws noted above and increasing vigilance of securities exchanges and security exchange commissions which are provincially run in Canada.

Implication of Policy Changes

Given the business critical nature of IT security and the increasing levels of legislative concern, the corporate response to such security drivers appears to remain tactical. As shown in Figure 6, only a minority of companies have created specific executive positions of responsibility for security and privacy⁴. Approximately 30% of Canadian companies have created these positions, roughly mirroring the performance of that in other countries. As such, it puts into question if these companies truly perceive security and privacy issues as strategic, given that the majority continue to make the responsibilities a component of another executive's overall functions.

⁴ As this is the first year the question has been asked no trending data is available.

Interestingly, when looking at the vertical market data, 50% or more of high tech, telecommunications, government, professional services and utilities professed to have created a Chief Security Officer (CSO) position. None of the retail respondents had created such a position, despite the well publicized concerns about customer payment data vulnerability and losses. While slightly more companies have a Chief Privacy Officer (CPO) [32% versus 29%], the results indicate a wider distribution across the industries – likely driven by PIPEDA's increasing maturity.

Of the respondents only those in the Energy and Telecommunications sectors indicated response rates in excess of 50%, however every industry, except Natural Resources, had at least one company with a Chief Privacy Officer.

While these lower numbers, which indicate an absence of day to day responsibility for security and privacy, may be cause for concern, a silver lining does exist for those that have moved in this direction. 62% of CSOs and 61% of CPOs report to either the CEO or the CIO, giving them some level of independence and we assume authority to act. However, only one respondent indicated that the CPO reported directly to the board. With the increasing scale of security breaches and data thefts and inconsistent disclosure of such events, the existence and reporting structures of CPO and CSO positions bears monitoring; especially as boards of directors may seek to shield themselves from potential personal liability fallout in data loss suits.

Disclosure of Breaches, Threats and Capabilities

As noted above, while the United States possess state laws that mandate disclosure to the public when personal data has been compromised, Canada continues to lag in the adoption of such laws. Interestingly, an important step forward occurred in 2007 with 66% of respondents, the highest proportion ever and the third consecutive year of growth, indicating that they would admit, when asked, to having experienced a breach. 38% more companies indicated this year that they would disclose such breach than did last year. However, 34% of companies would continue to keep such a breach under wraps, potentially compromising the confidential data of their customers and

Figure 6 - Designated Executives for Security & Privacy

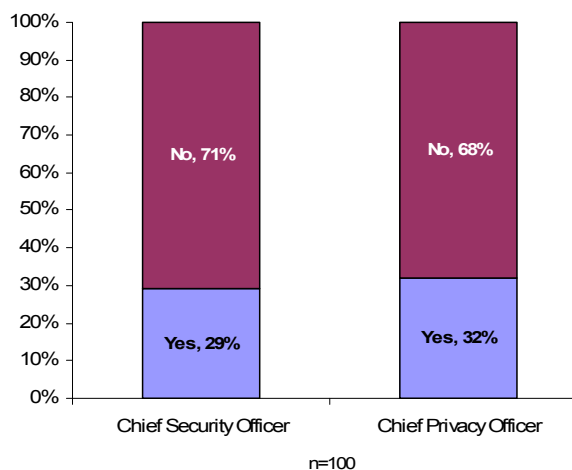
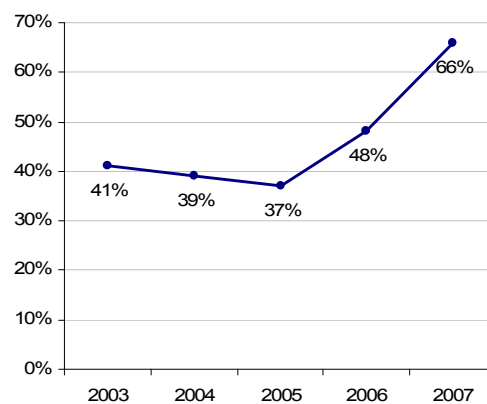


Figure 7 - Willingness to Disclose Breaches (2003 - 2007)



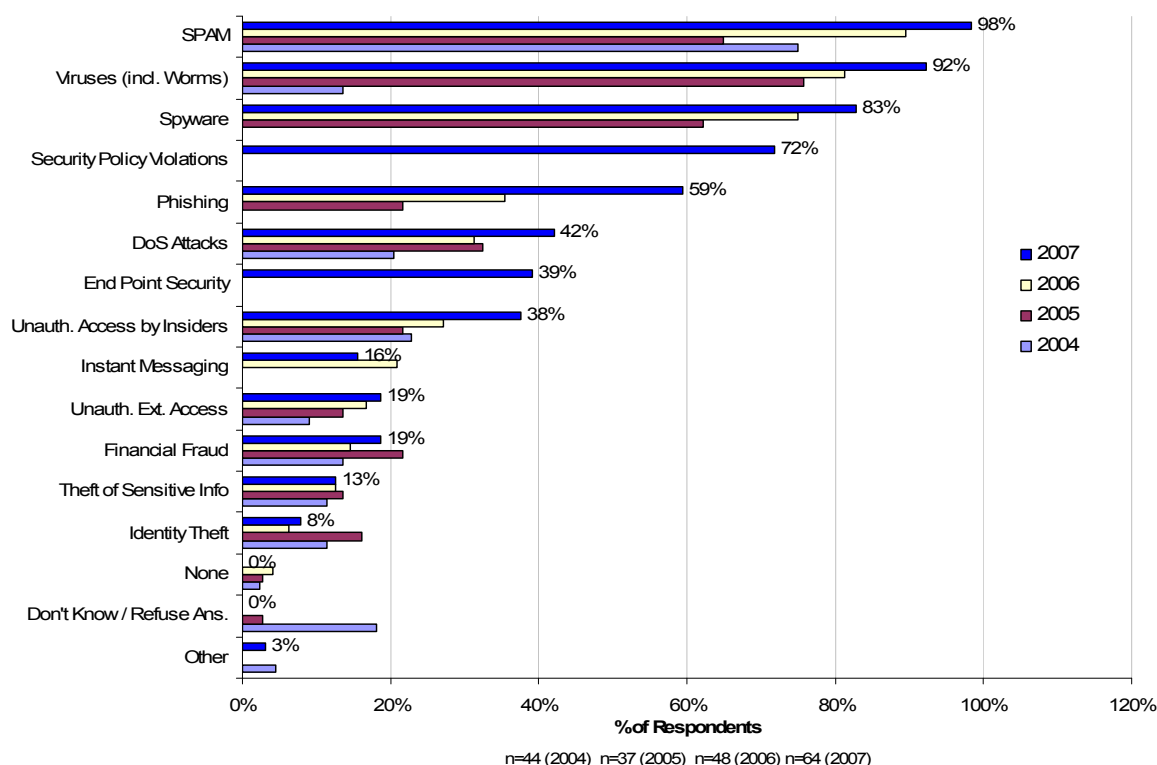
n=75 (2003) n=112 (2004) n=100 (2005) n=99 (2006) n=97 (2007)

business partners without their knowledge. This represents an interesting statistic given that in a recent CIO Magazine survey, 30% of Canadian companies admitted to not being in compliance with PIPEDA – although we note that Canadian performance in this survey was among the best in the world, which lends further credibility to this response level⁵. Until the enactment of tougher laws and precedents of tough sanctions exist, companies will continue to hide data loss events as the financial consequence could potentially cripple them.

Security Breaches

Companies experience the full gamut of security attacks from SPAM to viruses to phishing and pharming to security policy violation and endpoint security breaches.⁶ As noted last year, the intensity of such disruptions continues to increase across most categories of threat with **SPAM** and **viruses/ worms** being almost universal with 98% and 92% of respondents experiencing these security events, respectively. Given their existing dominance of the threatscape, the increases are proportionately small, although not insignificant (ranging from 8% to 10%). A similar scenario exists for **spyware**, the third most frequent breach type, with 83% reporting it. Strong growth emerges in **phishing**, which increased 69% to 59% (from 35% in 2006), and through **unauthorized internal**

Figure 8 - Security Breaches Experienced (2004 - 2007)



⁵ "The Global State of Information Security 2006". Allan Holmes. CIO Magazine. 15 September 2006.

⁶ Security Policy violation and end point security are new additions in 2007.

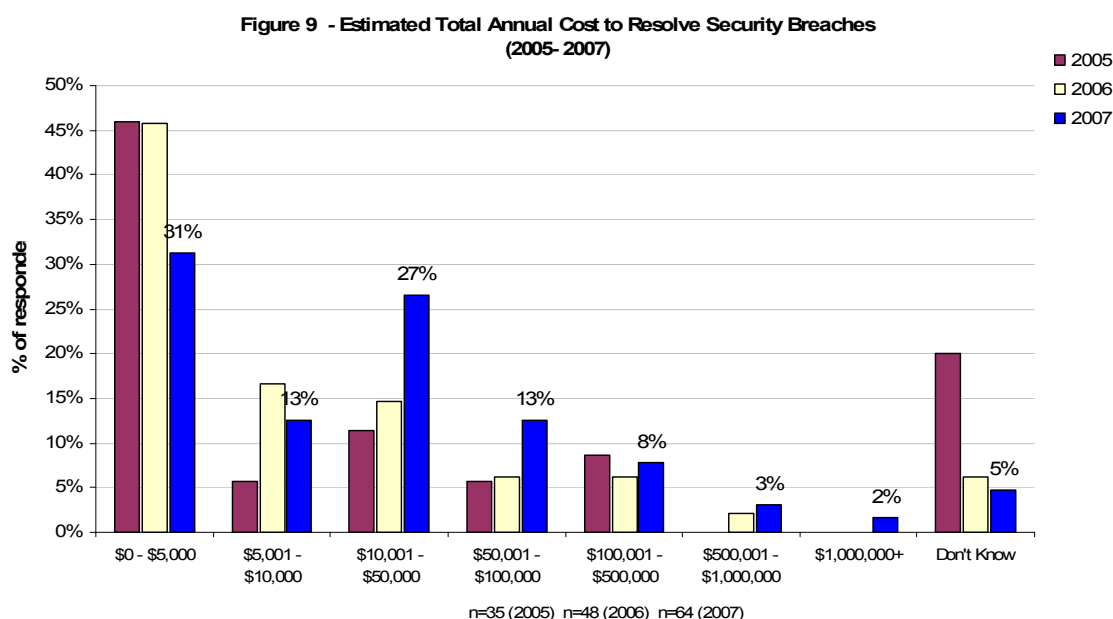
access, which increased 40% to 38% (from 27% in 2006). Both are alarming for different reasons. Increasing volume and sophistication drives the external phishing threat, while defending against unauthorized access by employees represents a whole different set of challenges from education to the highly sensitive issues (albeit increasingly accepted) of monitoring employee activities.

2007 introduces two new categories of threat: **Security Policy Violations** and **Endpoint Security** breaches. 72% of respondents indicated that employees have breached security policies in 2007, a clear indication that internal employee activities above and beyond unauthorized access require tremendous vigilance. At the same time, companies face proliferation of potential access points to corporate networks and data storage media (from USB memory sticks, portable back up drives, laptops and MP3 players) to permit employee productivity and remote access. Companies must now develop sound endpoint security plans and monitor them watchfully to permit a reasonable level of network access without compromising data - a difficult trade-off in even the most favourable environments. And in the case of endpoint security, even the best laid plans can be subject to errors. For example, CIBC mutual fund subsidiary Talvest lost a back-up drive with 470,000 client data records on it between its offices and an offsite back-up center.

The evidence of widespread and diverse forms of risk makes enterprise security one of the most hostile business environments. Potential enemies and threats lurk around every corner and range from the malicious to the ignorant.

Cost of Security Breaches

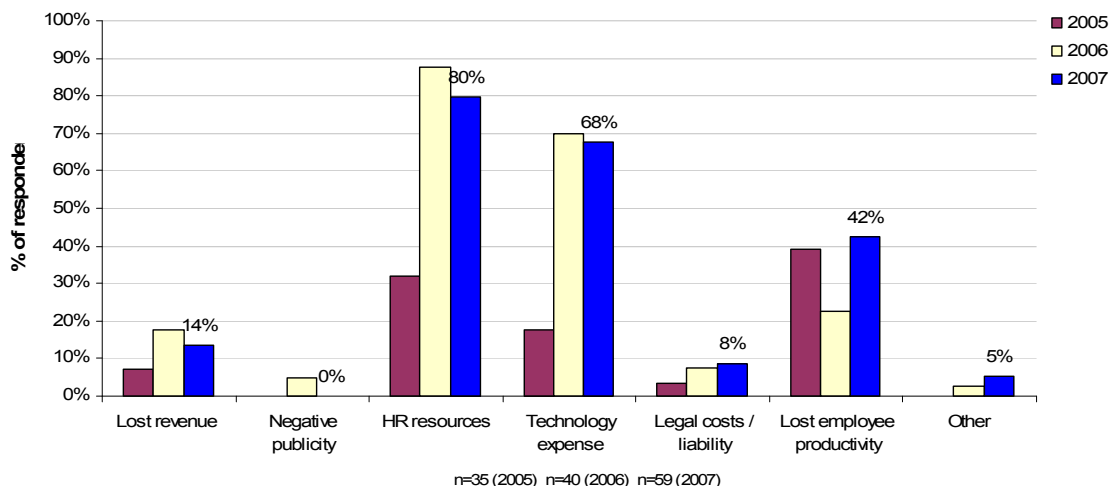
2007 demonstrates a trend toward rising overall costs in dealing with the combined annual security breaches experienced by companies, supporting the notion of increasing frequency and sophistication of attacks. Cost estimates at the low end (\$0 to \$10,000), while they aggregate to 43% of respondents, demonstrate an overall decline of 30% compared to 2006 levels, driven by fewer



respondents estimating annual costs in the \$0 to \$5,000 cost bracket. Moreover, all cost brackets above \$10,000 show significant growth, specifically mid-range costs, the \$10,001 to \$50,000 bracket, has grown 80% from 15% to 27% of respondents and the \$50,001 to \$100,000 has grown 117%, from 6% to 13% of respondents. Using the midpoints of each bracket as a notional cost of resolving security breaches, the cost to resolve security breaches has increased roughly 95% since 2005⁷.

As noted in Figure 10, human resource costs (80%) and technology costs (68%) comprise the most frequently cited costs included in the above amounts. Productivity losses also return to prominence this year with 42% (compared to 23% in 2006), although we believe that few companies possess the key performance indicator data that can accurately reflect a calculation of the true cost of disruptions, idle time and reduced efficiency. Similarly, other costs such as degraded network and infrastructure costs, eroded brand and shareholder value embody difficult to measure indirect costs that must all be factored into the security breach cost equation. We continue to believe that the majority of companies underestimate the true total cost of security breaches.

Figure 10 - Primary Costs Cause by Security Breaches



⁷ While not an accurate depiction of the actual median or average costs, using the mid-point of each bracket multiplied by the percentage of respondent per bracket derives a notional index. While this is skewed by the larger upper bracket, it provides an overall direction of cost, which is clearly increasing.

Threat Levels and Ability to Manage Threats

Given the challenges posed by the ever increasingly sophisticated and wide array of IT security threats, for the first time in the history of this study, the 2007 threat index has surpassed the level of 5 (on a scale of 1 to 10), as seen in Table 1. This penetration of the inflection point indicates that respondents believe they are more at risk, rather than less at risk, due to a security breach. This data is somewhat at odds with the data presented earlier

indicating less priority toward security and a stabilizing level of concern, although we must note that at an index value of 5.07 (median 5), the index only marginally exceeds 5.

The capacity to deal with this continually increasing risk (as demonstrated by consistent growth in the threat index since 2003), appears to have stabilized at a relatively comfortable 7.08 in the capability index. This number is consistent with the median result of 7.

The industry data looks relatively evenly distributed, with no one industry feeling overly threatened or over confident.

- Retail ranks above the median and index on the threat scale at 5.5 and below on the capability index at 6.6.
- Utilities and energy companies rank among the lowest in perceived level of threat and are inline with overall averages for level of capability.

Canada's Threatscape

Unsurprisingly, the range of threats facing Canadian companies remains relatively unchanged since last year in terms of the types of threats faced:

- viruses, worms, and blended threats;
- polymorphic threats (malicious code that can be manipulated and changed to prevent detection and change its function);
- botnets (or "zombie army" multiple computers that without the knowledge of users are infected to forward malicious transmissions on a large scale);
- external unauthorized access (hackers and crackers);
- unauthorized activities by insiders (intentional or 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");
- targeted attacks;
- SPAM, spyware and adware, and many others.

As indicated in the Symantec Internet Security Threat Report – Trends for July – December 2006, the intent of threats continues to change, with hackers increasing the focus for maximum impact and

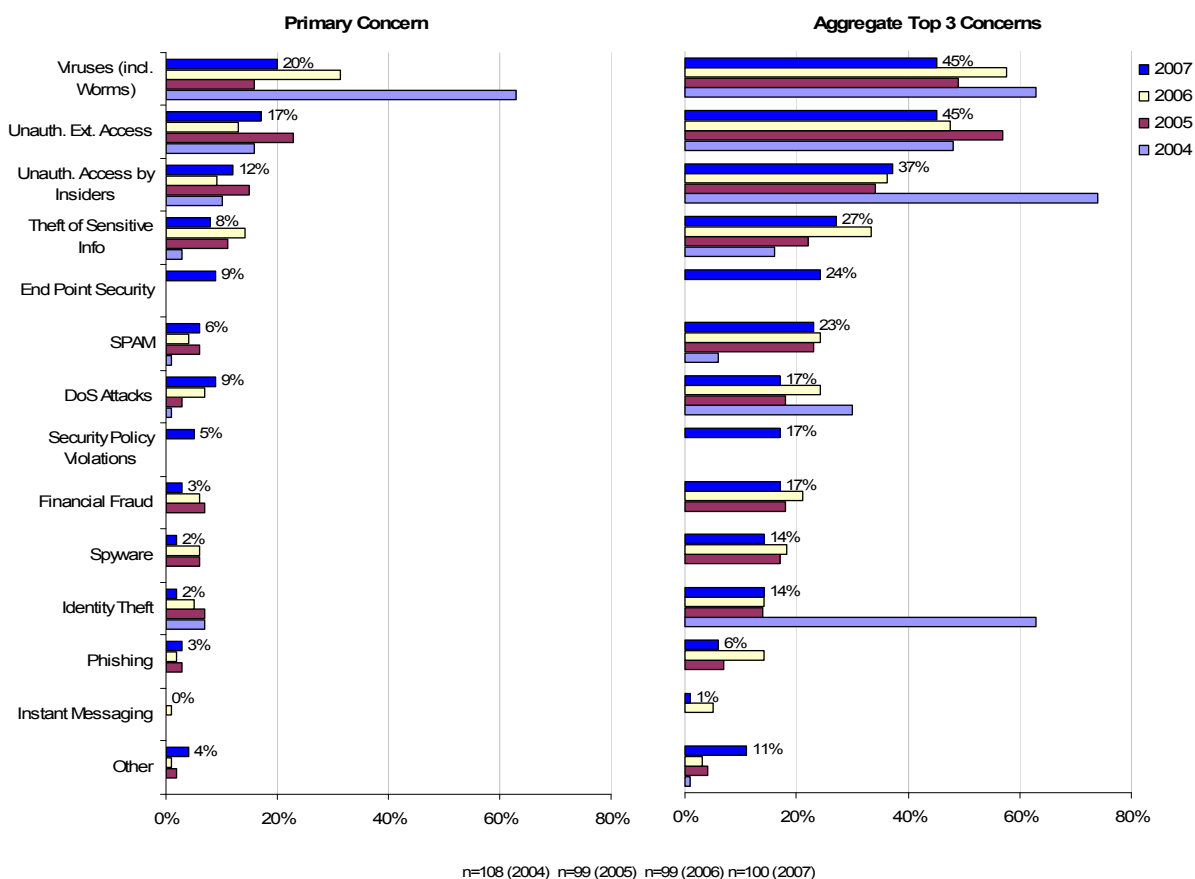
Table 1 – Threats & Capabilities

Year	Threat Index (1= Low; 10=high)	Capability Index (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

2003 n= 73; 2004 n= 108; 2005
n= 100; 2006 n= 100 2007 n =98

financial gain. Increasingly the intent of malicious activity appears to focus on data theft and the targeting of specific organizations for financial gain as opposed to “hobby hacking”. Moreover, instead of attacking through the deployment of a single threat instance (i.e. a standalone virus), hackers collaborate and strategize to create interoperable threats that may combine several threat types in a single attack. For example, a web application’s vulnerability may be exploited to permit the installation of bot programs that in turn spawns a key stroke logging application or phishing sites, potentially within the confines of a corporate network. Moreover, bot networks are increasing in scale and becoming more consolidated in nature. Coupled with the fact that they can be updated with new functionality and have adopted new, peer-to-peer and encrypted HTTP (as opposed to traditional IRC) communications protocols, security managers face a formidable threat.⁸

Figure 11 - Ranking of Threats
(2004 - 2007)



2007’s data indicates that little has changed in the 2005 to 2007 time frame with the overall ranking and relative proportions of concerns remaining similar (Figure 11). Nor does any one industry sector appear to have a specific concern about any particular type of attack. However, the responses

⁸ "Symantec Internet Security Threat Report – Trends for July – December 2006" Volume XI, March 2007.

appear to contradict managers' perceptions that they are at the highest risk level ever of being attacked. Perhaps the answer to this lies in the fact that the polymorphic nature of attacks makes any single type of threat less relevant. This creates significant implication from a defence perspective as companies must seek to deploy more integrated and coordinated solutions and processes.

Viruses and **unauthorized access (internal or external)** continue top the list of concerns, both as the #1 concern of security managers and in aggregate as top 3 concerns. Of note, both viruses and unauthorized external access have declined overall as top three issues and in the case of viruses substantially from 58% to 46% (a 20% reduction). In fact, viruses have also declined significantly as the #1 concern from 31% to 20%, while both unauthorized internal and external access have increased as #1 priorities for more respondents. This tends to support the premise that viruses themselves comprise less critical threats than the resulting access breaches that could comprise data and system and that significant threats continues to exist within the proverbial "four walls" of the corporation. As a dichotomy to this premise, concern over **theft of sensitive data** (a possible outcome of a breach or unauthorized internal access) has declined as both a #1 priority (from 14% to 8%) and in aggregate as a top 3 priority (from 33% to 27%), although it remains the fourth highest concern overall.

Endpoint security (a top three concern for 24%) and **security policy violations** (a top three concern for 17%) represent smaller, albeit significant, problems. They exceed the well known issues of **spyware** (14%), **identity theft** (14%), **phishing** (6%) and **instant messaging** (1%). **SPAM** remains a middle of the road concern and it is uncertain if IT managers have placed a high enough priority on this highly visible form of malware, especially given its ability to be a vector for other forms of attacks.

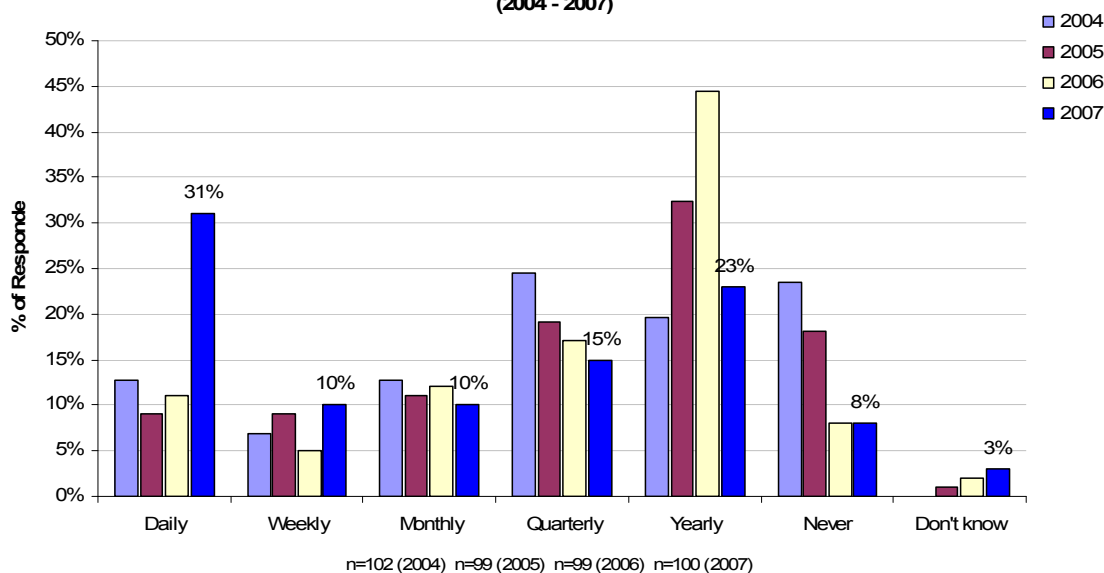
Last year, instant messaging and wireless were flagged as potential threats to monitor. Based on the responses this year, few respondents believe significant risk exists with instant messaging. Only 1% of respondents indicated it was among their top three concerns. This result likely arises due to the well documented vulnerabilities of the medium and the implementation of security policies that preclude the use of mass messaging applications like MSN Messenger and Yahoo! Messenger. Similarly, wireless concerns failed to appear as a key concern at all - an interesting result given that many experts believe the TJX data theft started through wardriving⁹ from a parking of a vulnerable store. The continued use of the more vulnerable Wired Equivalent Privacy (WEP) protocol for wireless encryption by many companies presents a threat from this perspective that needs to be recognized.

⁹ Wardriving is defined by TechWeb as driving around an area with a laptop computer and wireless LAN adapter in order to find unsecured wireless LANs. The goal is to find vulnerable sites either to obtain free Internet service or to potentially gain illegal access to the organization's data.

Viruses

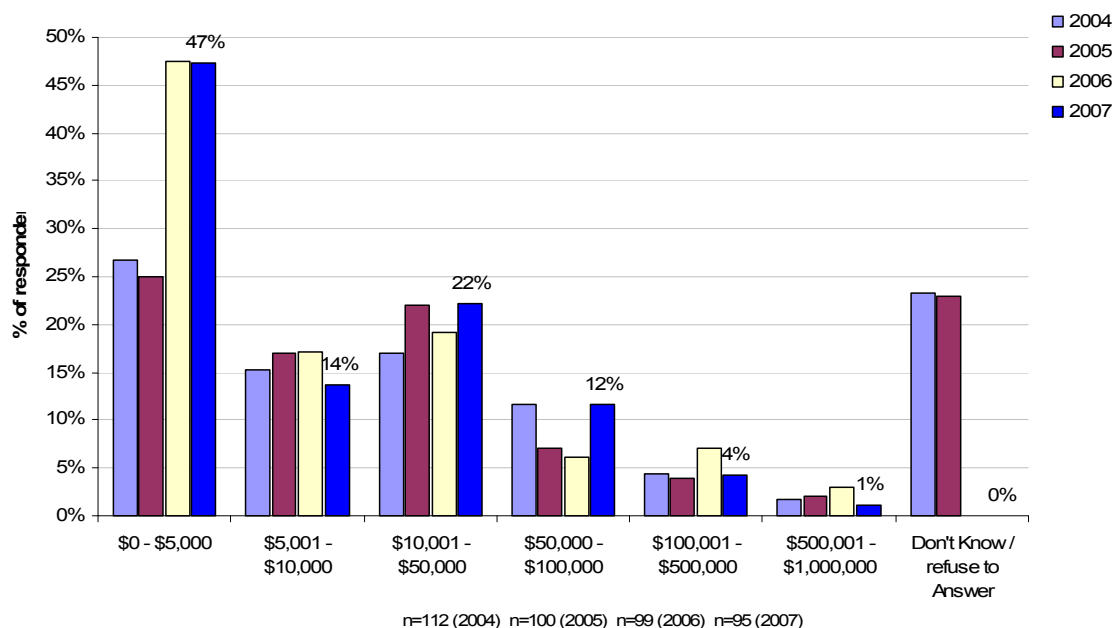
Unchanged from last year, viruses rank as the second most common form of attack experienced by respondents and, as noted above, is the top concern. Almost certainly, the disruptive nature of viruses due to the lost productivity, the cost to remediate and growing virus sophistication (i.e. morphing viruses that exploit application vulnerability and, like “superbugs”, become resistant to existing eradication tools) combine to create anxiety for IT security managers. Moreover, as seen in Figure 10, security managers report an alarming increase in the frequency of attacks with the number of respondents signifying that outbreaks occur on a daily basis almost tripling from 11% to 31%, radically reversing previous years’ tendencies toward less frequent outbreaks. Most of this augmentation came at the expense of those who reported only annual attacks (this proportion fell from 44% to 23% of respondents). While it seems difficult to believe that such a significant increase would occur since 2006, given the already high levels of infection noted last year, three forces may be at work: (1) more frequent attacks are being detected; (2) newer tools and processes allow for more rapid and effective detection of infections; and (3) increasing honesty of respondents.

Figure 12 - Frequency of Virus Outbreaks
(2004 - 2007)



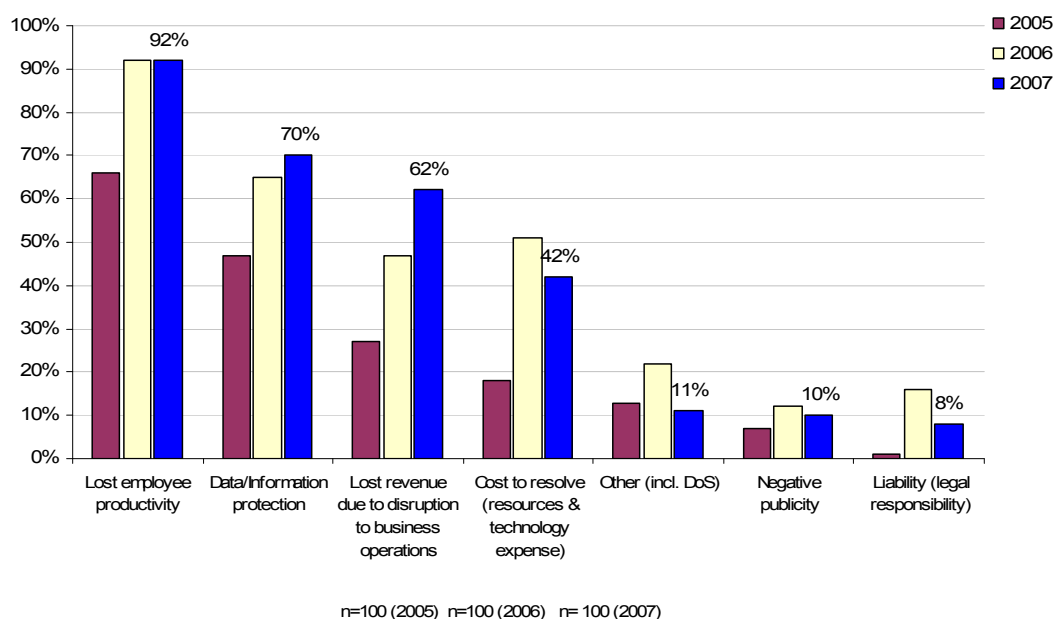
Distressingly, 8% of respondents report no infections. Financial Services companies represent half of these companies. This does not come as much of a surprise given that this sector boasts among the most strategic and advanced approaches to IT security. Its companies, more than any other sector, operate best in class infrastructures and employ highly sophisticated processes, given the strategic importance of data to their organizational performance and their position as trusted data managers of customers’ personal and confidential financial data. Similarly, utilities indicate only annual infections. Again, the fact that they comprise prime targets due to the financial nature of their assets and the mission critical nature of their services to the economy likely results in inherently more secure infrastructures through better design.

Figure 13 - Cost to Resolve a Virus Outbreak



As seen in Figure 13, virus outbreaks generally represent nuisance costs, with 47% of respondents declaring that a virus outbreak typically costs between \$0 and \$5,000 to rectify. However, 36% more also report costs between \$5,000 and \$50,000 – not an insignificant amount of money given the context of the increasing frequency of infection. It can be hypothesized that those reporting costs in excess of \$50,000 are those who have been subject to massive infections. Again, the financial services industry figures prominently among those reporting spending in excess of \$50,000 per incident to resolve outbreaks, lending further credence to the hypothesis that such organizations rank among the leaders in terms of data protection.

Figure 14 - Ranking of Top 3 Consequence of Virus Outbreaks (2005 to 2007)



Examining respondents concerns about potential virus infections (Figure 14), viruses cement themselves as disruptive nuisances above anything else. Consistent with last year, 92% of respondents include **lost employee productivity** among their top three hazards of a virus outbreak. This includes 51% of respondents articulating this as their #1 concern, more than double the next top concern – data/information protection. The decline in concern over the cost to resolve viruses (decline from 51% to 42%) may further characterize that companies are improving their ability to manage virus infections and are deploying automated tools that minimize the actual costs to remedy ensuing problems.

On the other hand, the continued climb of both **data/information protection** (70% in 2007 versus 65% in 2006) and **lost revenue** (62% in 2007 versus 47% in 2006 and only 27% in 2005) indicates a growing realization of the potential damage wrought by polymorphic threats, the increasing sophistication of targeted attacks for financial gain by criminal elements, and the potential resulting financial challenges for targets. Interestingly, despite these concerns companies appear relatively unconcerned with the possible negative publicity and liability resulting from a virus infection. This outcome points to a belief that possibly viruses present a lesser threat than other types of unauthorized access or as a result of physical data media loss with respect to their market goodwill and or the likelihood of being sued.

Securing IT Assets and Data

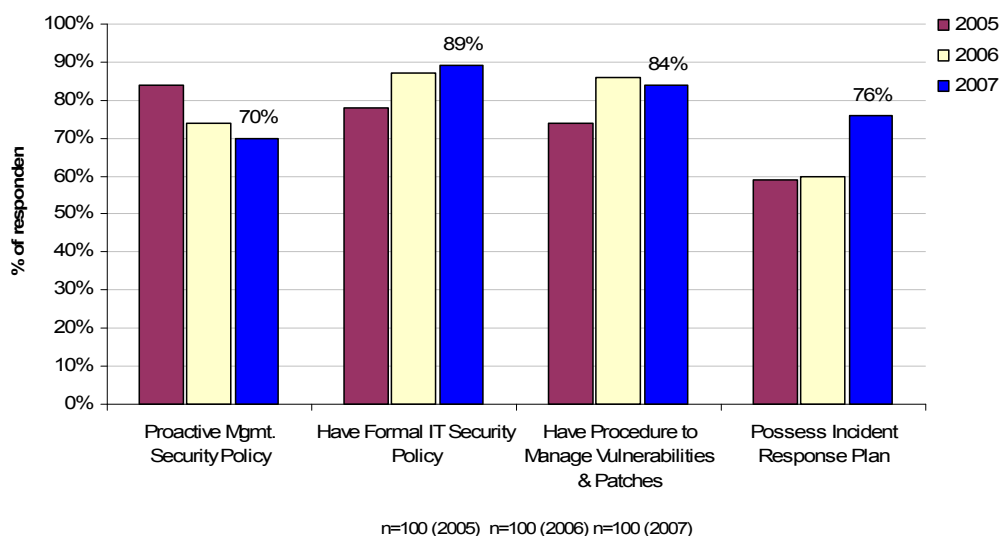
Strategic Threat Management

Many security pundits profess that companies employ reactive, tactical, silo-based approaches to IT security. However, a strategic approach to IT Security represents a critical transformation for IT organizations to undertake given the increasingly important nature of IT systems and data in delivering sustainable competitive advantage for corporations and their supply chain clusters. As a result, standards-based approaches like ISO 27001:2005 appear increasingly interesting and relevant¹⁰.

While last year there was a noted trend towards increasing strategic emphasis in building holistic IT security strategies, 2007's data paints a somewhat perplexing picture with fewer companies articulating priority focus on IT security (Figure 1) while continuing to invest broadly in process and technology. Moreover, 2007's data underscores a marginal but persistent decline in the proportion of companies that state they proactively manage IT security (70% claim this mode of operation in 2007 - down from 74% in 2006 and 84% in 2005).

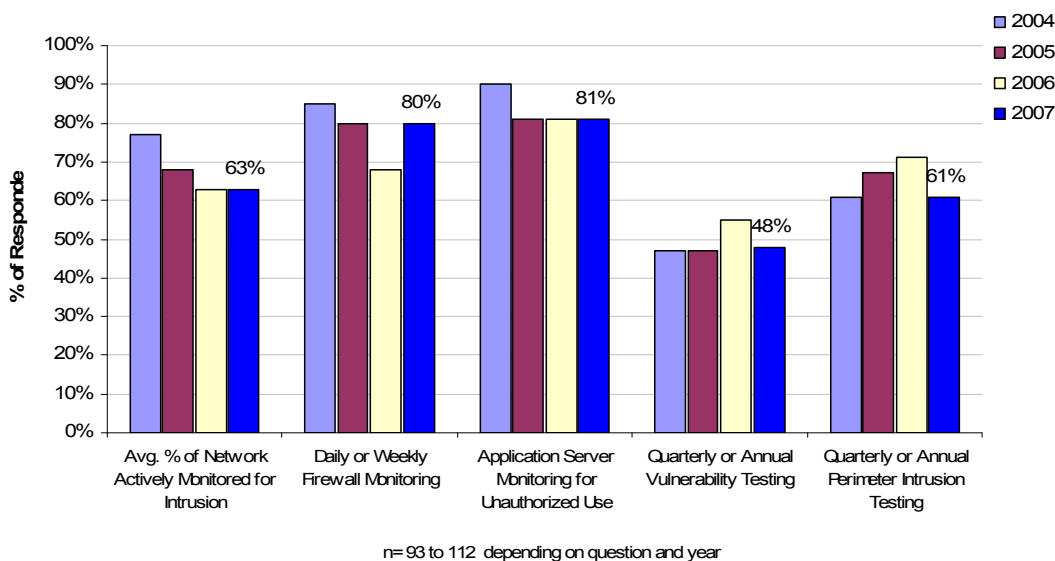
¹⁰ ISO 27001:2005 provides internationally accepted specification for Information Security Management Systems which is more wide ranging than many other frameworks.

Figure 15 - IT Security Policy & Processes



Despite these issues, there are a number of positive improvements in 2007¹¹. Given the intrinsically dynamic nature of threats, companies continue to embrace strategic processes to ensure corporate network and data integrity. Figure 15 shows that formal policies continue to become entrenched (and are clearly being monitored based on the number of violations being recorded) and more importantly, the proportion of companies that have created a formal process to respond to IT security incidents has increased 27% over 2006 from 60% to 76%. This result underscores the growing recognition that companies need not only deal with the technical issues of a security breach, but rather, that a complete, coordinated technical, legal and public relations management strategy may be required in the event of data loss to address the financial, liability and negative publicity issues.

Figure 16 - Security Processes Employed



¹¹This decline may simply be a function of the fact that security represents a combination of pre-emption and reaction.

When examining how other IT security processes are deployed, a consolidating pattern emerges as seen in Figure 16. Despite articulating a strategic view of IT security and implementing strategies designed to provide a more complete and holistic management framework, companies appear to bias their efforts toward reactive, tactical initiatives such as network monitoring for intrusions (63%) and frequent application server (81%) and firewall monitoring (80%) rather than pre-emptive activities such as vulnerability and perimeter testing which tend to be conducted on a quarterly or annual basis for most respondents at 48% and 61% respectively.

With respect to the processes deployed, the following characteristics exist:

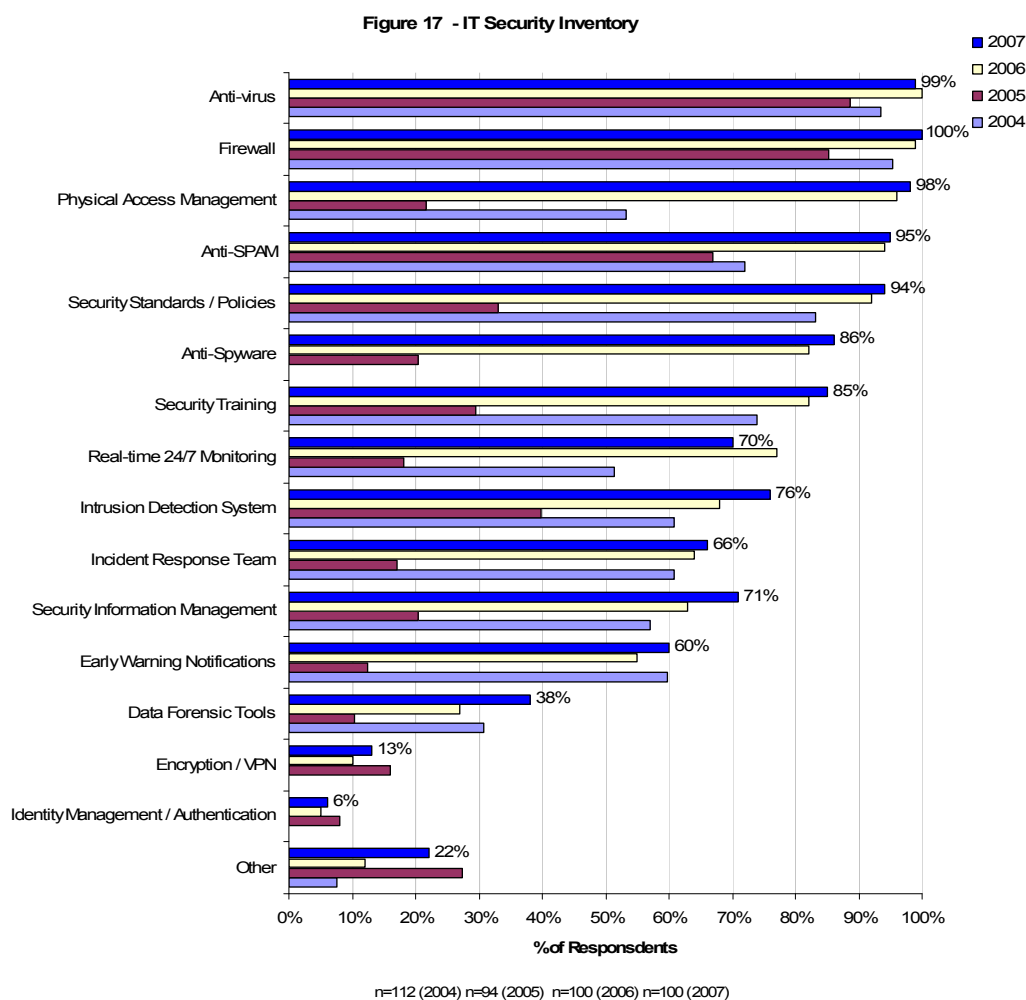
- **Active Intrusion Monitoring** – While on average companies monitor 63% of their total networks (unchanged from last year), only 27% claim their networks to be 100% monitored, a significant decline from the 41% who made that same claim in 2006. As such it begs to question if companies are having difficulty justifying the cost/benefit of such highly intense monitoring activities. Although not statistically valid, interestingly, financial services and retail respondents report among the lowest levels of average network monitoring at 52% and 38% respectively.
- **Firewall Monitoring** – Notwithstanding the continued trend toward de-perimeterization to provide business partner access to corporate data, firewall importance remains high to ensure the integrity of these extended networks. As a result, 62% of respondents monitor their logs daily and 90% do it at least weekly. Only 2% follow completely reactive processes and examine logs after an incident. Manufacturing respondents demonstrate a slight laggard tendency with the highest frequency of weekly or longer interval monitoring.
- **Application Server Monitoring** – 80% appears to be the equilibrium point for companies choosing to monitor application servers for unauthorized use. That this has not changed in three years presents an interesting statistic given the increasing prevalence of polymorphic threats that may enter as one form of attack but are changed into a botnet to leverage to the processing capacity of such servers. Sector analysis indicates that retail companies comprise those least likely to be monitoring these servers.
- **Vulnerability Testing** – This remains a more periodic practice with 26% conducting tests annually (2006 – 35%) and 22% quarterly (20% - 2006). However, the data points to a shift in responses to deal with increasing attack complexity. Weekly and monthly testing have increased in aggregate to 31% from 20% in 2006 and only 3% fail to test at all. No specific sector findings stand out.
- **Perimeter Intrusion Testing** – 44% carry out these tests annually (down from 54% in 2006). This positive change results in companies increasing their frequency of testing on a monthly, weekly and daily basis (15% versus 6% in 2006). However, it is concerning that 16% of companies perform no testing at all. Manufacturing companies appear most likely to engage in such testing given the potential for possessing extended supply chains and the potential devastation of a plant shutdown if production control systems become infected.

Partner Audits - A new element introduced this year, respondents were queried about their experience in auditing business partners or being audited by a business partner or authorities with respect to security and privacy.

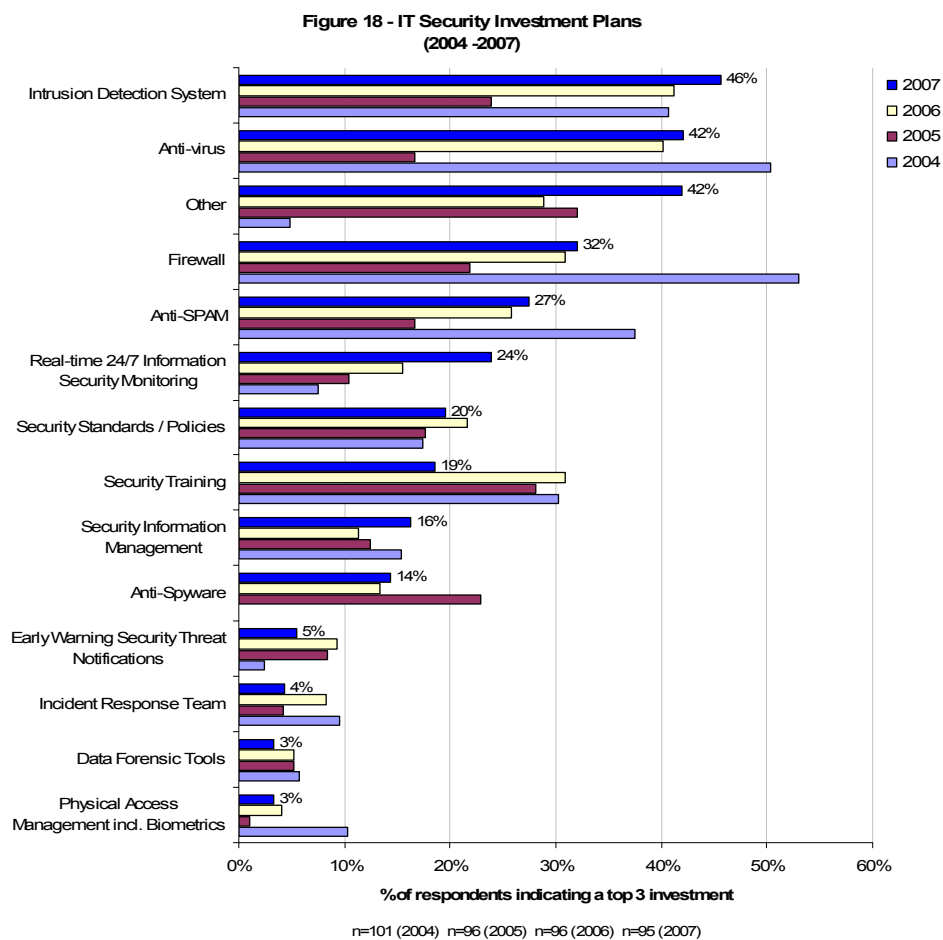
In general, the responses indicate marginally higher rates than previously. 54% of respondents indicated they were auditing their partners more frequently, while 51% felt that they were being subjected to audit more frequently. Given the increasing inter-company collaboration and integration required for success in the global supply chains and the rather limited involvement of Canadian companies in such value chains to date, it is expected that this number might increase in future surveys.

Tactical Threat Management

Symbolic of the increasing maturity of organizations' IT security investments, corporate inventories of tools and processes continue to be built-out, but from an already relatively mature level. Figure 17 provides an overview of the currently deployed tools and processes. All major categories of tools and policies exhibit growth, albeit at much reduced levels from previous years, due mainly to the pre-existing levels of investment. Clearly, given the noted concerns over viruses and unauthorized access, **anti-virus** (99%), **firewalls** (100%) and **physical access management** (98%) boast near complete deployment within respondent organizations. Trailing slightly, **anti-SPAM** (95%) and **anti-spyware** (86%) measures have been deployed by the majority indicating the concern over the potential costs of eradication of such attacks and the potential hidden payload that such infections may contain – given their increasing morphing ability and increased use of encrypted communication between bot infected computers and their command and control servers.



While little to moderate penetration growth is apparent, only one category revealed a decline in responses this year, **real-time 24/7 monitoring**, which declined from 77% to 70%. While the reasons remain unclear, a possible answer lies in the cost of such monitoring relative to the perceived benefit, especially given the increasing maturity and automation of tools and processes designed to deal with attack attempts. Alternately, it may also be an admission that security managers continually play a game of catch up with intrusions and the cost of such monitoring for some simply does not make sense.



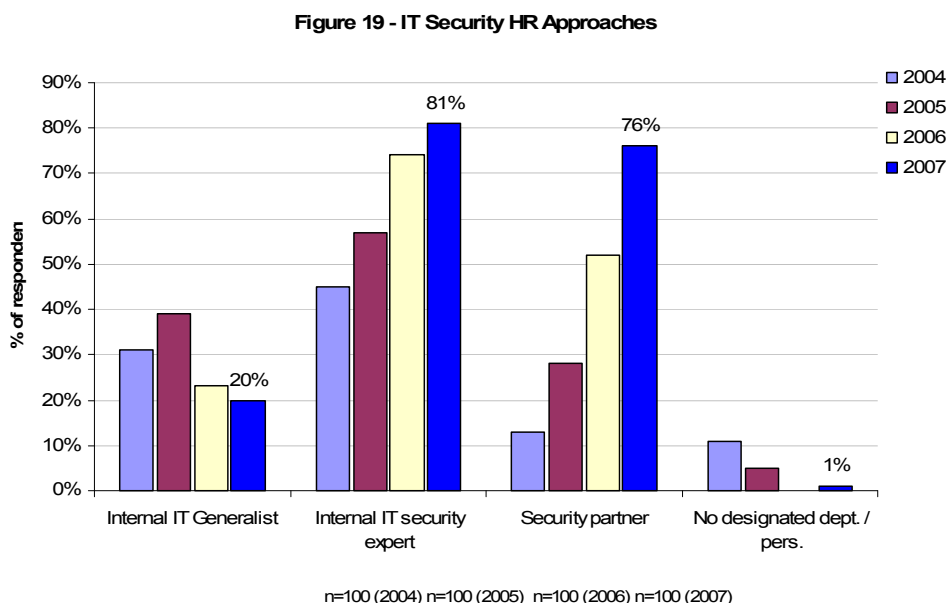
Despite the relatively comprehensive defence arsenals, companies continue to invest in an effort to keep abreast of the constantly changing threatscape. Figure 18 outlines future spending plans which emphasize continued investment in **intrusion detection** and **anti-virus** systems and processes. IT executives perceive both as critical core systems, with anti-virus technologies offering among the highest returns of any technology investment¹². A larger number of "other" priorities are noted as well. These tend to be company specific and range from such issues as business continuity and content management to endpoint security, data encryption and identity management. The challenge for companies in making these investments lies in ensuring that deployment does not occur in silos

¹² "2007 Vital Signs". Computer World. 1 January 2007.

that defend against specific and limited threats. Rather they need to be integrated and automated as part of an overall IT security strategy that unifies security management policies and data (much in the way network management tools do) to minimize enterprise risk. The growth in **security information management** may symbolize entrenchment in some organizations of this philosophy.

IT Security Resourcing

As data and systems continue to increase in importance from a competitive advantage perspective, focus on specialization becomes paramount in dealing with innovative and determined attackers. Respondents no longer trust their IT security needs to multi-tasking IT generalists as shown in Figure 19 with only 1 in 5 claiming to employ generalists down from close to 40% two years ago¹³. More than ever, companies rely on a combination of experts and third-parties to secure their data and networks, with 81% employing their own experts and 76% leveraging relationship with 3rd party technology and services providers.



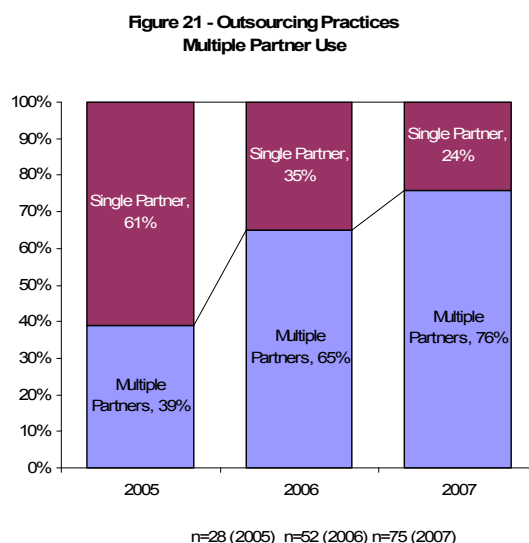
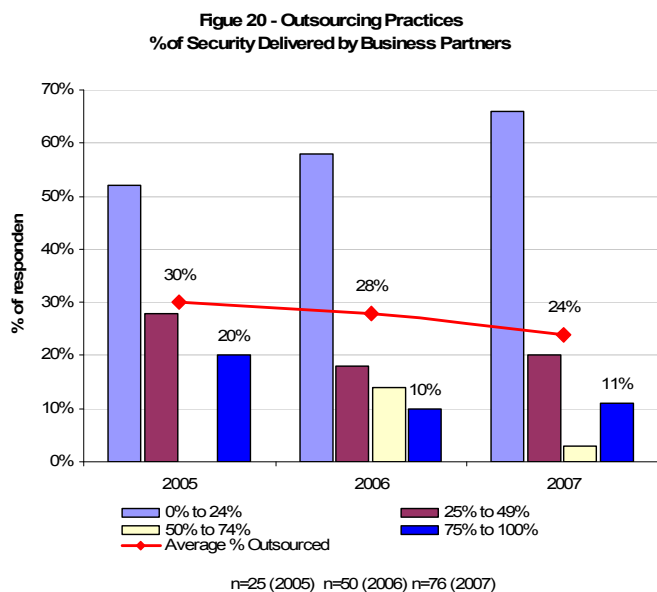
While the incorporation of business partners into the overall approach to managing IT security continues to grow significantly (growing 46% in 2007 from 52% to 76% of respondents indicating that they use third-parties), the data also yields that companies tend to be quite focused and selective in their use of a partner. Figure 20 highlights that on average the amount outsourced is typically under 25% of overall needs, and trends point to an overall decline in the total amount outsourced from 30% in 2005 to 24% in 2007. This trend bears continued watching. The issue does not appear to be client dissatisfaction with suppliers, as the overall satisfaction index continues to climb, albeit marginally, each year from an overall 7.43 (2005) to 7.69 (2007)¹⁴. As such, given the

¹³ Note - respondents selected all that types of resource that applied.

¹⁴ Index is calculated on a scale of 1 to 10.

increasing tendency to use multiple partners (Figure 21), one might conclude that corporate security managers seek to maximize the value of their security spending by focusing on buying best of breed services from partners that boast particular specializations or that they seek to ensure performance and reliability through redundancy and complementary services.

Industry-specific characteristics of interest include:



- Energy companies possess an inclination to outsource a larger percentage of their security more than others, while telecom and government respondents tend to maximize the use of inhouse resources.
- Use of multiple partners appears to be reasonably spread out among all industry sectors, although energy, manufacturing and financial services tend to have the largest proportions of respondents indicating the use of multiple partners.
- Levels of satisfaction appear the same regardless of industry with most being close to the above noted index number.

IT Security Spending Trends

Very little change relative to IT security spending is noted over the survey's history. Median spending remains firmly established at 5% of most corporations overall IT budgets (an entirely consistent result when compared to the 2004 to 2006 period). This represents an area of concern as the results point to a persistent trend that Canadian spending on IT security fails to keep pace with that of our US neighbours. US companies report spending reached

Table 2 – IT Security Spending as a % of total IT spending

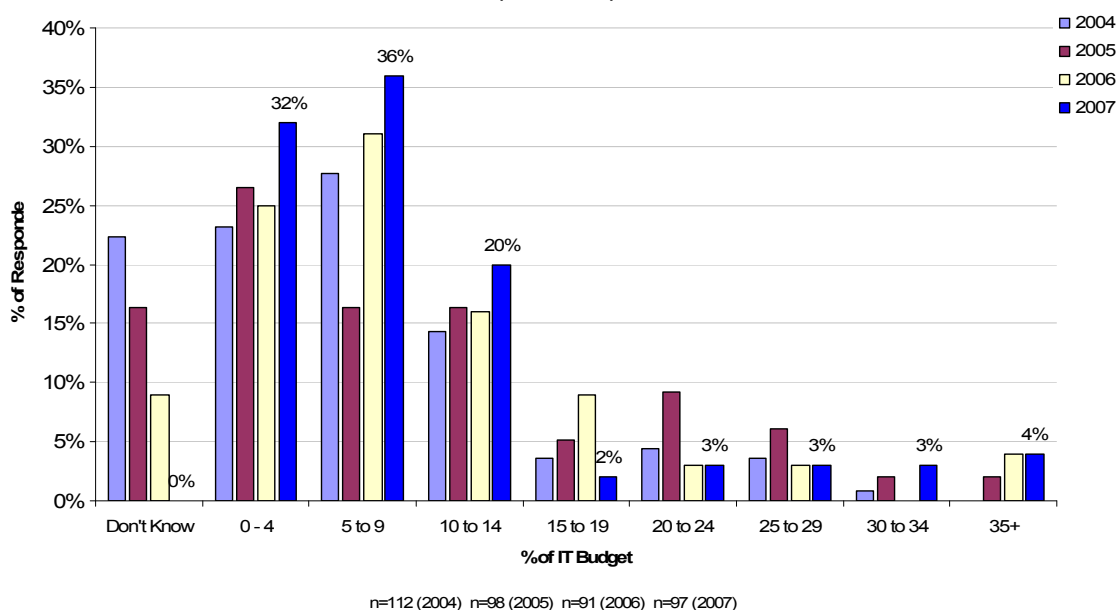
Year	Median	Average
2004	5%	7.6%
2005	6%	10.1%
2006	5%	10.0%
2007	5%	8.5%

2004 n=87 ; 2005 n= 82; 2006 n= 91; 2007 n =97

17% of total IT spending in 2006¹⁵. This growing gap places Canadian companies at risk of being disintermediated from trading relationships due to the perceived incremental risk of doing business.

Examining this spending from a different perspective, Figure 22 reveals that the bulk of budgets (68% in 2007 compared to 56% in 2006) remain concentrated under 10% of overall technology spend. However, a persistent group of companies (4%) remain outliers, spending well over 40% of their total IT budget on security. As these do not appear in consistent sectors from year to year, one can only surmise that these companies have specific issues that require such an unusual level of spending, whether it consists of specific investment projects or the need to protect unusually sensitive data and systems. Additionally, from a sector perspective, most sectors tend to fall between the median and the average in terms of overall spending. Not surprisingly telecommunications companies lead the way with respect to overall spending on IT security, given the recent data that revealed that 92% of all identified bot infected computers can be found in this sector's computers¹⁶. Retailers tend to lag comparatively.

Figure 22 - Proportion of IT Spend on Security Products & Services (2004 to 2007)



¹⁵ "The Global State of Information Security 2006". Allan Holmes. CIO Magazine. 15 September 2006.

¹⁶ "Symantec Internet Security Threat Report - Trends for July - December 2006" Volume XI, March 2007.

Budget Allocations

Budget allocations among staff cost, training, technology (hardware and software) and consulting remain virtually unchanged since last year. Software and hardware appears stable at just under 40% of overall spending. Staffing costs have fallen marginally from 33% to 31%, but slight increases in training and use of consultants absorbs this decline. These increases support the aforementioned notion of specialization being sought in IT security skill sets.

Figure 23 - Allocation of IT Budget

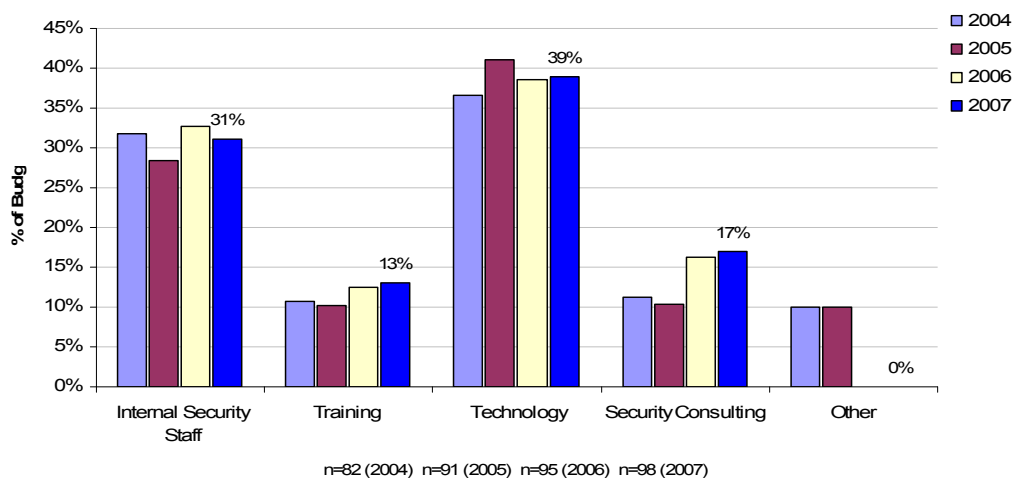


Figure 24 (a) - % Indicating Belief in Spending Increases

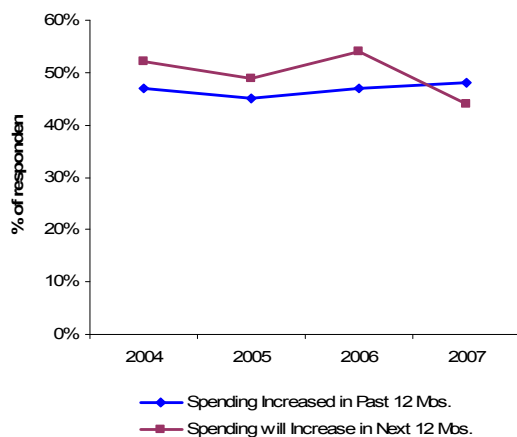
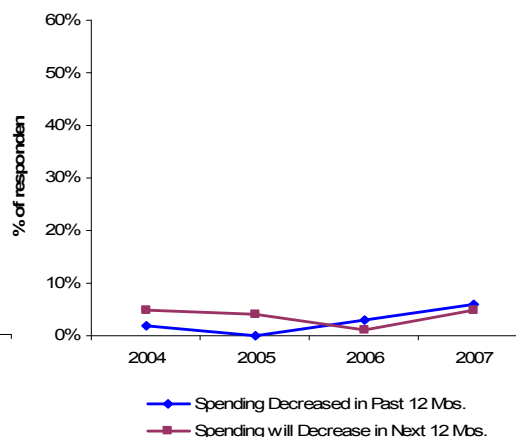


Figure 24 (b) - % Indicating Belief in Spending Decreases



n=106 (2004) n=99 (2005) n=100 (2006) n=100 (2007)

Spending Trends

IT security managers' perception of security spending appears steady to growing with 94% of respondents indicating that the last twelve months witnessed stable to increased levels of spending and 95% expecting stable to growing spending in the next 12 months. These numbers appear optimistic when compared to the median and averages presented above which paint a relatively static picture for spending over the last four years – one can only presume that overall IT budgets continue to grow in absolute dollar terms to permit this continued growth in IT security spending.

An interesting observation this year lies in the fact that for first time respondents indicated the highest percentage ever of belief that budget shrank last year, albeit with only 6% of respondents making this assertion (Figure 24(b)). Coupling this data point with the fact, that for the first time in the survey's history, future spending optimism has fallen below the past year's perception of spending growth (44% versus 48%) and that the highest proportion ever (small at 5%) believe that budgets will shrink in the coming year, indicators point to the potential for weaker IT security spending in 2007. The data may reflect that companies are wrapping up major investments in IT security or simply be coloured by industry analysts' belief that overall spending growth will be scaled back in 2007.

Conclusion

At the risk of sounding cliché, the statement "*the more things change, the more they stay the same*" aptly describes the IT security landscape and provides the key theme to sum up the data from this year's survey. Threats continue to proliferate, all the while becoming more complex, sophisticated and well-targeted with viruses representing the most critical threat reported by IT security managers. The mainstreaming of malicious hacking as a criminal enterprise appears to be the rule of the day. IT security managers continue to respond with a combination of strategic processes and policies, by creating IT security expertise through training and sourcing it from 3rd parties and by investing in automated tools to keep pace with increasing threat innovations and thereby prevent intrusions and data loss.

Generally, Canadian IT security managers appear to feel reasonably comfortable with their ability to meet the challenges imposed by an ever changing threatscape. And meeting them head-on represents an imperative task. More than ever, IT systems and data represent critical, strategic assets in building and sustaining a position of competitive advantage in today's globalizing marketplaces.

Within this context, 2007's respondents create a dichotomy. While IT security managers feel increasingly at risk of attack, fewer companies are making IT security a top 5 priority. This result presents an alarming situation that we can only hope is anomaly. More than ever, corporations face an exposure to significant financial penalty for failure to secure key data and systems. Additionally, companies face the challenge of increasingly distributed and mobile working environments, inter-

company systems integration and the proliferation of mobile personal devices (Blackberry's, laptops, USB flash drives, MP3 players, etc.) that can connect to corporate networks. As such, endpoint security represents a growing issue for IT security managers to address.

Under such circumstances, data security and detection and prevention of unauthorized access lie at the top of mind for most respondents. As a result, not only are companies investing in process and technology to meet these needs, they increasingly engage security experts and turn to expert 3rd party service providers to tap their specific security expertise. The potential financial losses, losses of revenue, erosion of shareholder value and potential legal liability for failure to prevent unauthorized access to, and disclosure of confidential data, require such levels of specialization. The requirement for such focus can only increase as legislative requirements continue to move toward mandated public disclosure of security breaches that put personal and customer (or business partner) data at risk.

Frequent (daily in many cases) and almost universal infections by various malware types compound these strategic, potentially business interrupting, risks. SPAM, viruses, and spyware, the most frequently reported types of malware, erode employee efficiency and effectiveness and consume valuable IT human resources. As such, it is not surprising that key spending priorities lie in intrusion detection and anti-virus tools to minimize disruptions. Moreover, within this story of challenge we find solace in the fact that companies appear to have the cost of remedying these nuisance issues under control as their policies and processes become more structured and sophisticated, and automated, integrated tools are deployed. This being said, the majority see the cost of responding to security breaches climbing, most probably due to the sheer volume in attacks.

Despite this situation, the data does not indicate significant IT security spending growth (certainly not more than overall IT spending growth), with average spending on IT security services and products hovering between 8% and 10% of total corporate IT spending. Moreover, certain indicators point to a potential softening of spending going forward. This represents a cause for concern given the increasing threat levels.

While last year demonstrated the strategic significance of IT security, the 2007 study shows a mixed set of messages and provides an overall tone that indicates a slight loss of momentum in strategic security adoption in Canada. Given the critical importance of data to building competitive advantage and in allowing Canadian companies to integrate themselves into global value chains, it remains imperative that Canadian companies maintain and enhance their **FOCUS** on developing robust IT security strategies and deploying integrated tools, policies and practices that promote the optimum levels of data, network and systems security.