

MARKET OPTIMISM BUOYS 2010 CANADIAN IT SECURITY OUTLOOK



3/5/2010

Findings from 2009 & 2010 MTI Research

Data from the 2009 and 2010 IT Market Dynamics *Market Tracking Initiative* buy-side research, complemented by insight from Canadian IT managers and vendors, shows how the outlook for IT security spending is changing in 2010.

EXECUTIVE SUMMARY

As we move into 2010, solutions play an increasingly-important role in Canadian IT market dynamics. Spurred by the involvement of line-of-business managers in the IT evaluation and purchasing process, IT buyers continue to focus on acquiring new capabilities, rather than upgraded core infrastructure products. In response, resellers and vendors continue to look for ways to wrap “building block” technologies into systems that address discrete buy-side management requirements.

There are a handful of solutions that have captured the attention of both buyers and sellers – mobility, virtualization, unified communications, and IT security. In many ways, the first three of these represent areas in which IT builds capabilities that are deployed against business priorities. IT security is unique in that the IT output – secure access to information – is also the desired line-of-business management outcome. The need to safeguard sensitive information, and to document the process for compliance purposes, extends across organizations of all sizes.

In our Market Tracking Initiative, IT Market Dynamics – the research arm of the IT in Canada network – has conducted more than 3300 surveys with Canadian “buy side” executives over the past 12 months. By comparing responses from 2009 with those collected in 1Q10, we are able to build an understanding of market trends in the Canadian IT sector – including for IT security. To flesh out this perspective, we have also conducted in-depth interviews with two firms that are intimately involved with the daily need for secure operations – The Grocery People and Invera – and with Mohammed Akif, Microsoft Canada’s National Security and Privacy Lead. Key points arising from this analysis include:

- Security spending will rise substantially in 2010. In 2009, approximately 26% of MTI survey respondents reported six month purchase intentions for security products. Looking ahead, we find over 40% planning new spending in 2010.
- The increase extends across all sizes of organizations, with the proportion of buyers large, mid-sized, and small enterprises all increasing by more than 40%.
- Users in Canada are embracing security technologies that provide robust protection for corporate data, including two-factor authentication and 128 bit encryption for VPN traffic.
- Canadian companies, according to Microsoft’s Akif, “have realized that the cost of not investing in security is significantly higher than in getting the security process right, getting their people trained, and investing in the right technology. If they are not able to do that or if they put that on the back burner, then the resulting damage to their goodwill, to their reputation, to their sales, is significantly higher.”

OPTIMISM BUOYS SECURITY OUTLOOK

IT Market Dynamics is still in the process of evaluating its 2010 forecast data, but our preliminary results indicate that 2010 will be a year of renewed focus on security products.

Through the course of 2009, we surveyed more than 2400 Information Executive subscribers, to stay connected with the pulse of the Canadian IT sector. Preparing for 2010, we are again surveying thousands of our print readers, and also reaching out to new contacts across Canada to gain additional perspective on market trends. Thus far, we have completed more than 900 surveys with Canadian IT executives to understand 2010 budget priorities.

Based on analysis of this research, we are confident that there will be a substantial upsurge in IT security purchases in 2010. Although our comparisons between years aren't perfect – in 2009, we asked for six-month purchase intentions, and in the current period, we are asking about intentions for the full year of 2010 – the overall direction of our findings is clear. As is seen in Figure 1, purchase intentions within each size category are substantially higher for 2010 than they were for 2009. Weighting this data by the relative product purchasing power of the different e-size categories, we find that a total of 41% of Canadian purchasers plan to invest in security products in 2010, vs. an average of 26% reporting six-month purchase intentions in 2009.

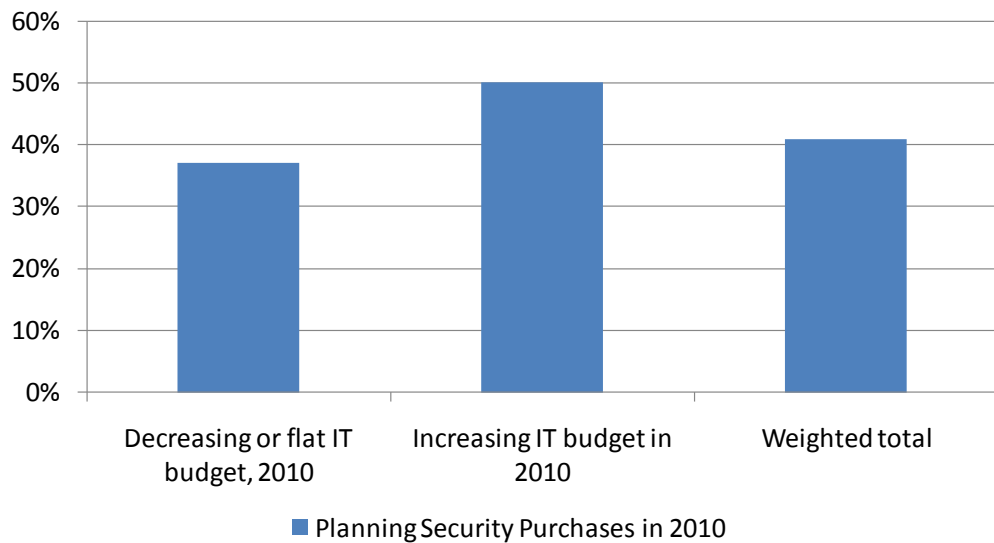
FIGURE 1. PURCHASE INTENTIONS FOR IT SECURITY PRODUCTS, 2010 VS. 2009



It is evident that the recovering economy plays a major role in this increased activity. Looking at weighted results from our 2009 research, we see that only about 15% of Canadian accounts were forecasting increased IT budgets for last year. Our preliminary 2010 research indicates that this proportion has doubled, to about 30% of Canadian IT buyers expecting increased funding for

2010. While many Canadian IT managers were willing to invest in security even in spite of decreasing budgets last year, the improving outlook has led a much higher proportion of buy-side executives to earmark funds for security purchases in 2010. If confidence in the business community continues to increase through the course of 2010 – as was the case towards the end of 2009 – investment levels in security products could rise still further. As Figure 2 illustrates, fully half of IT managers with increasing budgets are planning new purchases of IT security in 2010; if their ranks swell with improved economic news, we can expect to see overall IT security investments increase as well.

FIGURE 2. 2010 SECURITY PURCHASE INTENTIONS BY 2010 IT BUDGET TRENDS



CANADIAN CASE STUDIES

Through the course of our research, we had the ability to discuss security practices and purchase intentions with three knowledgeable Canadian experts:

- Roger Osness, IS manager, The Grocery People
- Pierre Masse, data centre supervisor, Invera
- Mohammed Akif, National Security and Privacy Lead, Microsoft Canada

The balance of this paper presents the “lessons learned” from these conversations.

The Grocery People

From the outside, you wouldn't necessarily guess that The Grocery People Ltd. (TGP) in Edmonton considers itself a potential target for electronic thievery. But according to the folks in this grocery wholesaler's information systems (IS) department, the firm takes data protection seriously.

"There's a threat there," says Roger Osness, IS manager.

Owned by Federated Co-operatives Ltd. in Saskatoon, TGP offers grocery, dairy, frozen, confectionary, fresh produce and meat products, serving small and mid-sized grocery retailers from the west coast to western Ontario. It operates its own distribution centre in Edmonton, and non-food distribution centres in Calgary, Saskatoon, and Winnipeg.

Asked if the 500-person company sees itself as a security target, Osness says it does. The firm plays an integral role in the electronic purchase infrastructure (pin pads, card readers) that its customers use at the till. TGP supplies the technology that gets transactions from clients' counters reconciled with credit card companies' and banks' back-end systems.

The small food retailers that TGP serves have been pegged as potential targets themselves: according to the Payment Card Industry (PCI) Security Standards Council, small firms are more at risk than large companies when it comes to data theft, Osness says.

"Probably the reason for that is the big ones would pay more attention," he says. Large companies often have more resources to apply to information security than small businesses do.

So it's up to TGP to ensure that the transactions making their way from the retailers' counters to the financial institutions are protected.

The company uses point-to-point VPNs between its head office and each retailer, says Wes Rau, the systems analyst.

"We use AES 128 encryption on that tunnel," he says.

Unemployment tempts good guys to try on black hats

Organized crime has an easier time recruiting smart technologists when the economy is bad, says Microsoft Canada's national security and privacy lead.

It's a terrible time to drop your investments in IT security, notes Microsoft Canada's National Security and Privacy Lead. According to Mohammed Akif, the state of the economy could be putting organizations at a greater risk than they'd face in a better economic environment.

In an interview with Michael O'Neil, president of IT Market Dynamics Ltd., Akif says organizations need to be watchful these days.

"There are more people available in the job market that can be approached by organized crime, or by hackers. It's an environment where people might be desperate to make money. Therefore it becomes even more important for companies to ensure that their IT infrastructure is safe and their customers are having a secure computing experience."

For the most part, Canadian firms seem to understand the risks – and they're working to mitigate them, Akif says.

Continued

The Advanced Encryption Standard (AES) operates at three protection levels: 128 bit; 192 bit; and 256 bit. Even at its lowest level (128), it would take a sophisticated computer nearly 150 trillion years to crack, according to the U.S. National Institute of Standards and Technology (NIST).

It isn't foolproof, however. Security experts have discovered "side channel" attacks that could compromise an AES-protected system by focusing on the computer infrastructure associated with the encryption. And last year, researchers developed an attack that would move AES cracks from the realm of the impossible to that of the theoretically possible. Still, industry observers say AES remains an excellent protection mechanism that thwarts real-world attacks.

TGP uses SonicWALL Inc. firewalls in its security infrastructure. The vendor "had a fairly good following in the retail segment already," Rau says. "It was one of the only ones that offered a dial-up failover."

That's important for retailers in remote locations, Osness says. "Reliable Internet is quite an issue in a lot of our locations."

TGP recognizes a shift in the payment card industry that sees theft liabilities being pushed from card providers to retailers. Initiatives like the PCI Security Standards Council help retailers – and wholesale partners such as TGP itself – take on the data-protection responsibilities.

"They're kind of forcing us to pay attention," Osness says. "Eventually any liability because of an intrusion would be owned by the stores themselves, and not the credit card companies."

Invera

While some companies choose unified threat management systems to cover all of their security needs, Invera Inc. takes the "best of breed" approach, acquiring point solutions for firewall, antivirus, and access management. This way, the company's IT decision makers feel sure that their information is best protected.

"The problem with all in usually is... they tend to be generic and... very expensive," says Pierre Masse,

"Companies have realized that the cost of not investing in security is significantly higher than in getting the security process right, getting their people trained, and investing in the right technology. If they are not able to do that or if they put that on the back burner, then the resulting damage to their goodwill, to their reputation, to their sales, is significantly higher."

IT Market Dynamics – the research arm of the IT in Canada network – has found via surveys with Canadian IT decision makers that 45 per cent of firms with increasing IT budgets are planning near-term security investments. Akif says that from his experience, many of those organizations are looking beyond point solutions for 2010.

In the past, "spending more on security meant buying another intrusion detection system or upgrading their firewalls....Now we have seen that people are realizing that security needs a holistic approach. So I do find that the companies that are increasing their budgets are actually investing on looking at the security policies, looking at how they apply patch management, how they assess a patch, how to determine if a new security patch should be applied

Continued

data centre supervisor at Invera, a Montreal-based software company specializing in ERP systems for the steel and metal industry. “They’re not necessarily the best in all categories, so we rather try to go for the best fit for us for each category.”

Unified threat management solutions entered the market about five years ago, offering a contained security platform that handles information access procedures and gateway functionality, to help keep viruses and other external attacks out of the corporate network. Benefits include simplified integration – when all of the security systems are combined, organizations ostensibly face less hassles to make the components work together. That often translates into lower operating costs, and an opportunity for the IT department to allocate funds for other technology projects.

But while a number of organizations have chosen the unified route – combining their VPN, content filtering and anti-spam systems – others such as Invera prefer a more individual route. Best-of-breed proponents often say it’s worth the extra integration work to use the top-of-the-line products, because they feel that the individual technologies work better than the combo options.

In Masse’s environment, access management is the heart of the security platform. For nearly a decade, Invera has used a two-factor authentication system from RSA, the security division of EMC Corp. The system features both a user PIN and a SecurID authentication token displaying a six-digit code that changes every 60 seconds.

Users need both the PIN and the current code to access the network. “This way, if somebody knows my password but they don’t have my SecurID, they can’t get in,” Masse says. “And vice versa: they may have my token, but if they don’t have my PIN, they can’t log in either.”

Masse says the IT department works with business decision makers on selecting the components of the information-security system. The company has just 85 employees, and it’s a technology provider itself, so the business leaders and the technologists work more closely

and what the time frame should be for it.”

Organizations are also investing in people to ensure that their IT infrastructure is designed securely. Noting that many of the security issues that organizations face happen at the application level, Akif says he sees increased attention paid to software security.

“So we did see people realizing the importance of investing in, for example, training their developers to ensure that they come up to speed and they know the basics of how to write programs that are secure by default or secure by nature.”



Mohammed Akif, National Security and Privacy Lead, Microsoft Canada

with each other than they might do in other organizations.

“Our upper management is very hands on,” Masse says. “They’re kind of technically savvy in the first place. They tend to drive most decisions and the kind of things they want to protect themselves against.”

The firm aims to protect its intellectual property and its customer details against theft, for competitive reasons and as a matter of trust. Invera takes its security stance seriously, although the company doesn’t see itself as a specific target for hackers.

“We get a lot of spam,” Masse says. “So that’s a threat, maybe. But no, I don’t feel we’re targeted by anybody else.”

ABOUT IT MARKET DYNAMICS

IT Market Dynamics is a full-service IT research company operated by the IT in Canada network partners, including Information Executive, CRN Canada, and Canadian Government Executive magazines, and the web network that includes the sites for each of these publications, as well as GreenerIT.ca, UC in Canada, the IT Forum Exchange, The Efficiency Platform, ROI Innovation, Secur-IT, and IT in Canada.

For more information on IT Market Dynamics, please contact us at info@itmarketdynamics.ca