Determining How Much to Spend on Your IT Security

The Canadian Perspective

An IDC InfoDoc | 2015

IDC
Analyze the Future

Introduction

Organizations struggle to determine how much to spend on IT security, an investment many liken to insurance — no one wants to pay more than they have to. This IDC report offers guidance for setting the appropriate size of your security budget as well as helping to weigh the growing options from on-premises to managed services to cloud. IDC profiled Canadian organizations' security investments alongside their success and failures as a baseline for others to draw comparisons to their own activity. The findings in this study are from 2015 IDC research conducted in Canada.

Canadian organizations say they spend an average of just under 10% of their IT budget on security technology, outside services and staff. How much an organization invests in IT security stems from a range of criteria. Organizations that are consumer facing, that have a large attack surface, a recognized brand, highly guarded intellectual property, and compliance requirements to industry regulations and government legislation tend to outspend their peers. The reality is, though, that organizations of all types have experienced security breaches. There remains a misplaced belief in "security by obscurity" among organizations with lesser known brands, smaller attack surface, and less stringent industry regulations.

Canadian organizations say they spend an average of just under **10%** of their IT budget on security technology, outside services and staff.

Your Security Budget In Perspective

IDC studied the budgets, recent breaches, maturity levels, and several other key criteria of over 200 Canadian organizations, and found that four distinct security profiles emerge. The following diagrams illustrate the wide gulf between organizations that perform well and get a high score on IT security versus those with weak security. Not all organizations are created equal — and their security investments will vary — but the gap between the haves and the have-nots should be narrower.

Defeatists

This group of organizations suffers from poorly funded IT security. Under funding and sub-par planning have caused more damage by making them more vulnerable to security breaches. They are "defeatists" because IT/security stakeholders/ professionals tend to stop lobbying their executives for support. Manufacturing and primary industries lead this profile, but IDC finds examples of all industries and sizes of organizations here too.

Denialists

These organizations have moderately funded IT security, but have poor security practices. Their real challenge is that they often don't recognize how bad the situation is. They are more likely than average to suffer data breaches, yet they retain a high degree of confidence in their security prowess. One tangible problem they have is too much focus on buying the right technology and not enough focus on security skills/training and processes for better risk management. Public sector, telcos, and other industries and organization sizes are among organizations in this profile.

Realists

These organizations are doing a fairly good job at IT security. They may, in fact, be overspending and wouldn't know it. They don't spend enough time working through a formal risk management process to properly assess and measure their ongoing performance for a given amount of investment. Retailers lead this profile, but are found among the Defeatist and Denialist profiles as well.

Egoists

These are the security elites. They have spending in line with risk, suffer fewer breaches, focus on recruiting and retaining top notch security professionals, and have achieved a high degree of maturity across people, process, and technology. Their only potential Achilles' heel is an unwavering confidence. It may be justified — but hopefully it doesn't reduce vigilance. The Canadian banking and financial sector leads this profile. There are examples of public sector and service provider organizations within this profile as well.

Your Security Budget In Perspective (continued)

	Defeatists	Denialists	Realists	Egoists
	Their IT security is weak and underfunded	Their IT security is weak but they lack full awareness of this reality	Their IT security is fair and they strive to be better	Their IT security is good but they risk over-confidence
Percentage of organizations	23%	37%	23%	17%
Breaches compared to average	More	More	Fewer	Fewer
Percentage of IT budget on security	6%	8%	14%	12%
Confidence in security defenses	Low	High	Low	High
Focus areas	Trial and error/ little risk process	Technology over people/process	Employee training/ benchmarking with outside peers	Formal risk process/hiring topnotch staff
Level of maturity out of 5	1–2	2–3	3–4	4–5
Industry profile	Manufacturing/ resources	Public sector/ infrastructure/ telco	Retail/ distribution	Finance

Current spend on IT security

9.8%

of IT budget

IDEAL spend on IT security

13.7%

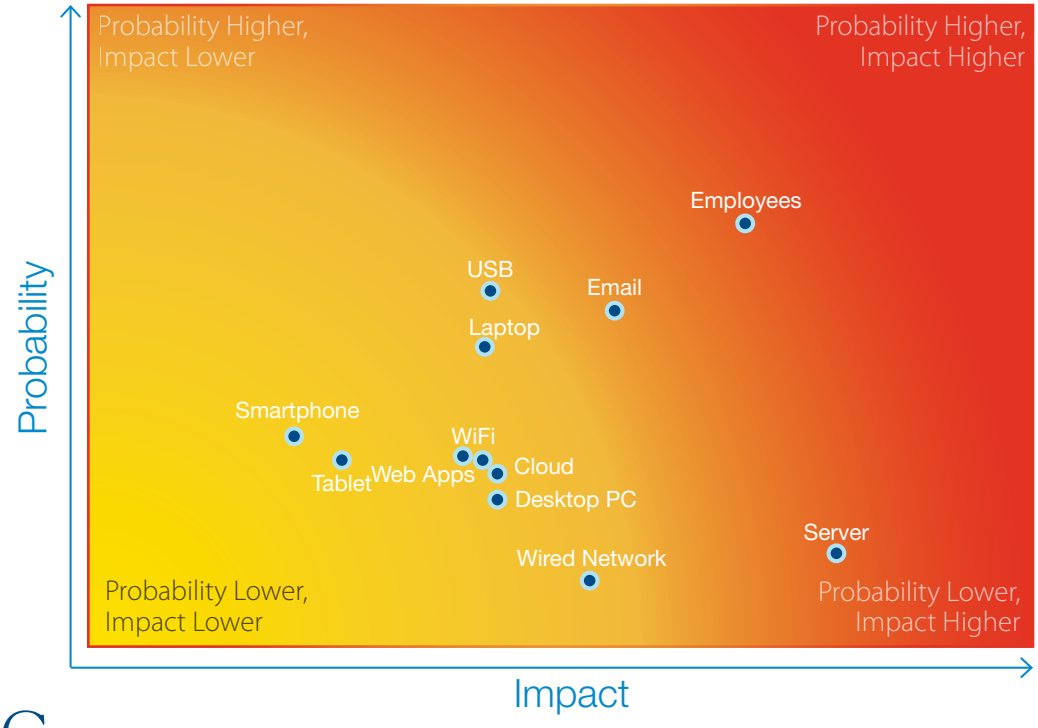
of IT budget

In the midmarket, IDC notes a higher than average budget growth through 2015 for IT security — and this is good news for a market segment in particular need of improved security.

IDC recognizes that for some organizations the security budget is not part of the IT budget. We use total IT spend as a common benchmark to apply in most cases.

Directing Dollars Where They're Needed Most

IDC asked Canadian organizations to rate the likelihood that their various physical assets and human resources could be compromised and to assess the consequences of this. It is striking how tablets, smartphones, and web applications are not considered more strongly as points of security weakness, which leads to underinvestment in these areas.



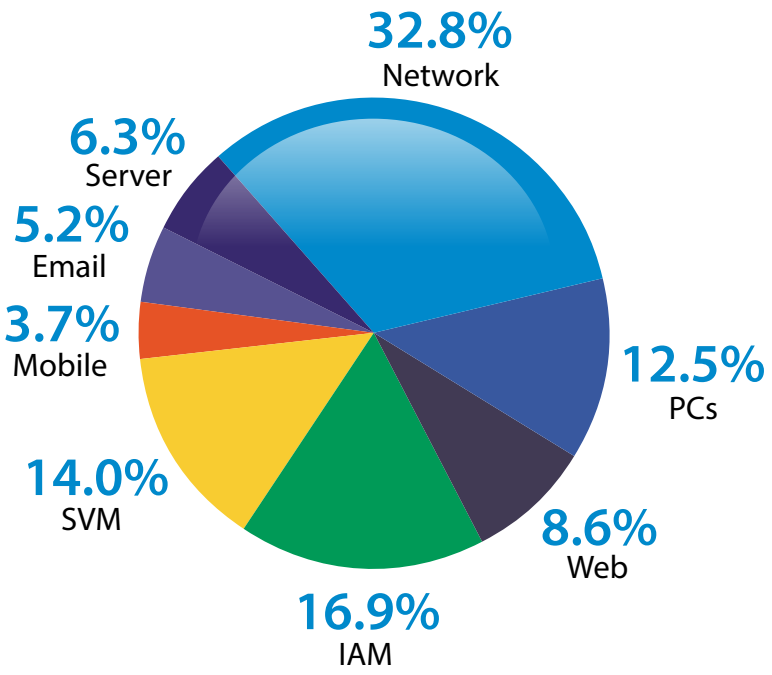
It is striking how tablets, smartphones, and web applications are not considered more strongly as points of security weakness.

Directing Dollars Where They're Needed Most (continued)

Employees are cited as a security weak link. Many organizations would like to allocate a bigger share of the security budget toward employee training (primarily in departments outside of IT such as sales, marketing, and HR). On average organizations would like to spend a significant 24% of their IT security budget on building best practices, awareness, and education. The reality is that shoring up employee lack of security knowledge will continue to be carried out on much less than this percentage.

For a different perspective, IDC added up all security products purchased in Canada across eight different categories to provide insight into how the average Canadian organization is distributing its security budget. The figure to the right shows how this budget is distributed, based on which technology assets are being secured.

Distribution of Security Budget Across Eight Key Technologies



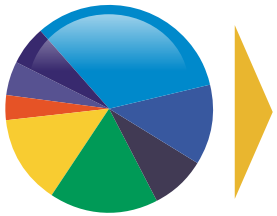
SVM: Security and vulnerability management
IAM: Identity and access management

Security Investments Becoming Less Traditional

There is a skills shortage in IT security — and it is reshaping the security market. Increasingly, organizations are filling the skills gap with managed security services and/or cloud security services.

The percentage of total security budget heading to the cloud shown in the figure below refers to securing traditional assets through the cloud rather than in the cloud. Over time, IDC forecasts high growth in Canadian security spend to secure applications and data running in the cloud. For example, organizations need visibility into traffic coming into and out of infrastructure, platform, and software as a service. Cloud providers do handle some security, but there are elements of data loss prevention, identity management, and so forth that your organization will continue to oversee.

Cloud has been a thorny subject in Canada owing mainly to fears over the Patriot Act, which permits U.S. law enforcement to compel disclosure of data held in a U.S. datacenter. The tide is turning, though, given that nearly 7 out of 10 organizations in Canada now indicate that cloud providers are more secure than their own IT.



Optimal Budget Allocation Desired by Canadian Organizations

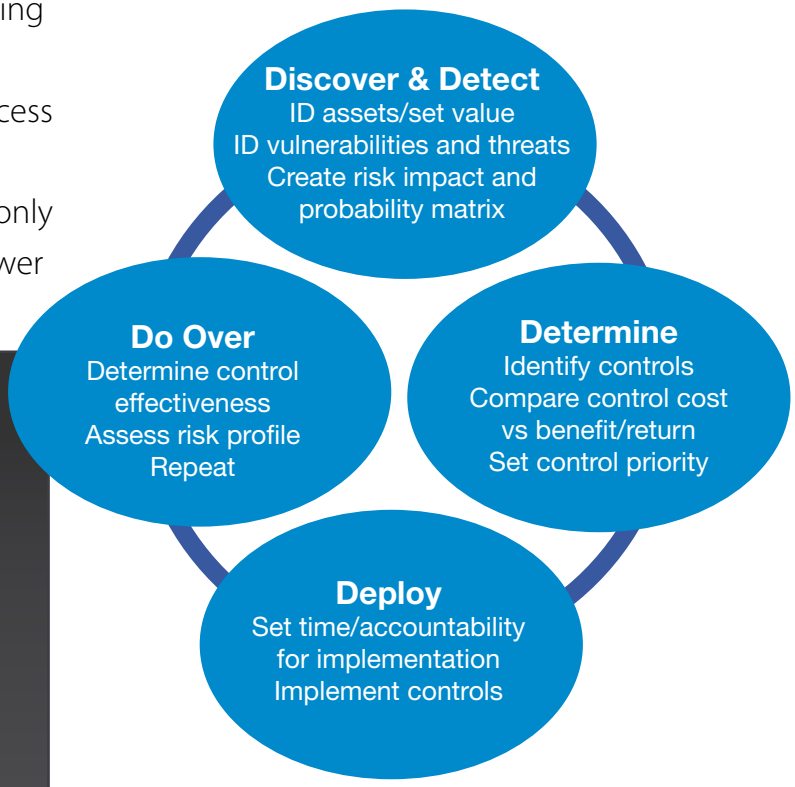
	Server	Network	PCs	Web	IAM	SVM	Mobile	Email
On-premises	82%	81%	73%	59%	57%	54%	51%	49%
Managed services	9%	11%	15%	22%	25%	29%	24%	25%
Cloud/SaaS	9%	8%	12%	19%	18%	17%	25%	26%

Working Out How Much to Spend on IT Security

The right answer does not start with a dollar figure, but rather that organizations work through a risk management process. However, most organizations take an ad hoc approach, basing their budgeting decisions on trial and error, or reacting to problems as they arise instead of proactively approaching a security framework. This process is monitored and repeated, and shortcomings are addressed over time. This simple (yet time-consuming) process is undertaken by only a third of Canadian midmarket and large organizations, and far fewer small businesses. The risk process is rather straightforward:

- ✔ **Discover** the inventory of assets (end user devices, applications, network devices, data repositories, supply chain/partners). **Detect** the vulnerabilities / weaknesses of these assets and establish which threats could compromise each
- ✔ **Determine** and prioritize your investments in technologies, skills, and processes (called controls and countermeasures). Base decisions on the probability / impact matrix from the Discover & Detect phase
- ✔ **Deploy** controls to shore up vulnerabilities across assets to defend against given threats
- ✔ **Do over** and repeat this process on an ongoing basis (at least annually) while measuring the effectiveness of your investments (preferably in real-time)

Simplified Security Risk Management Process



Planning Beyond the Fiscal Year

Set a multiyear plan to forecast how much progress your organization will make in security risk management, technology selection, security professional recruiting/retaining, employee training, incident response, and a range of other areas of focus. Set a baseline for security activity to establish a frame of reference for future progress. Organizations in our Realist and Egoist successful security profile categories tend to follow a measurable path to achieve higher levels of security than average.

Five-Level Security Maturity

Next Steps

- ✔ Set your security budget according to the cost of countermeasures/controls defined during your risk process
- ✔ Benchmark against organizations that have managed to keep breaches low while spending 12% of the IT budget on security
- ✔ Establish a multiyear plan to consider how your invested security dollars will pay off

Authors:

David Senf, Program Vice President, Infrastructure Solutions

Kevin Lonergan, Analyst, Infrastructure Solutions

Dave Pearson, Research Manager, Storage and Networking

Sponsor: IBM

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.