

**Nearly Unanimous Call for Increased Legal Liability on
Organizations That Store Large Quantities of Hackable
Customer Information**

**BDO Dunwoody Weekly CEO/Business Leader Poll
by COMPAS for publication in
the *Financial Post* February 5, 2007**



**COMPAS Inc.
Public Opinion and Customer Research
February 5, 2007**

1.0 Introduction

CEOs and business leaders are deeply concerned as both consumers and business people about the threats posed by the successful hacking into customer databases. Hacking won't go away, and hackers will maintain their lead, perhaps even increase it, over information protection systems.

Laws should be changed to assign greater responsibility to retail, banking, and other organizations that possess large amounts of such information. Such organizations should be legally required to inform their customers as soon as a penetration occurs, and they should be held legally liable for the financial impact on their customers as a result of hacking and identity theft.

These are the principal findings from the weekly business web-survey conducted by COMPAS for the *Financial Post* under sponsorship of BDO Dunwoody LLP.

2.0 Deep Concern for Panelists as Both Customers and Executives

CEOs and business leaders are deeply concerned about the threat of hacking as consumers and even more so as business executives, as shown in tables 2A and B. Some comments:

Identity theft is a major problem especially because anti-money laundering laws now require financial institutions to have so much personal information about customers including social insurance number, photo copies of passports, drivers license, birth certificates etc.



*Electronic Records Confidentiality, BDO Dunwoody Weekly
CEO/Business Leader Poll, by COMPAS for Publication in the
Financial Post on February 5, 2007*

I am very concerned that increased data theft and misuse of confidential information is going to grow, all across the world. Hacking is like counterfeiting. Our currency continues to evolve into a more complicated document to counterfeit and the counterfeiters become more and more sophisticated too. Hacking is a fact of life and overcoming hacking is an industry in itself. This issue won't get any better, it will just get more complex.

Table 2A: Degree of Personal Concern about Hacking as a Customer (7=serious concern)¹

Mean	7	6	5	4	3	2	1	DNK
5.4	25	33	22	8	5	6	2	0

Table 2B: Degree of Personal Concern about Hacking as Leader of a Business (7=serious concern)²

Mean	7	6	5	4	3	2	1	DNK
5.8	43	26	16	7	5	2	2	1

Panelists' depth of concern emerges from a perception that hacking will not recede as a threat, as shown in table 2C.

¹ (Q1) As you know, at least one of the major banks and a major retail chain had their customer records penetrated with these records subsequently used for criminal purposes. Some customer credit cards are at risk. On a 7 point scale where 7 means you personally are seriously concerned and 1, the opposite, how would you score your concern about electronic record penetration and misuse in your personal role as a customer?

² (Q2) How would you score your concern and that of your colleagues about protecting your organization's records against unauthorized access. Please use the 7 point scale where 7 means seriously concerned and 1, the opposite.



Table 2C: (Q3) There's some debate as to whether electronic records are inherently more vulnerable, especially when connected to the Internet, or whether hackers will always be several steps behind. Do you think that electronic record systems linked to the Internet will...ROTATE POLES

	%
Be increasingly vulnerable as hackers develop their skills	31
Remain slightly vulnerable, as they are today	52
Be increasingly safe and impenetrable as the barriers to unauthorized entry become stronger	17

3.0. Overwhelming Support for Increasing the Liability on Organizations

Given their expectation that hacking will not go away, panelists are concerned to protect both customers and business from its effects. With this in mind, an overwhelming majority of panelists believe that organizational holders of customer information should be increasingly liable for its protection under the law, as shown in table 3A. By an overwhelming margin, panelists also believe that organizations should be legally required to inform customers the moment their systems are successfully penetrated, as shown in table 3B.

Comments:

With identity theft on the rise and more and more personal data being stored electronically, it is beholden on those collecting the data to be continually updating their systems to prevent unauthorized access.

Credit card and personal information is used by many companies to conduct their day to day business affairs. Many people now use the web to buy products, as it is a simple and satisfying process. As such those companies that



do business through the web have an obligation to protect their customer's information. However, the government has an obligation to be of assistance by passing laws that will punish those that misuse this increasingly used tool very harshly to discourage others. That means they need staffing that can track and apprehend those people. As this happens within the global web, countries must work with each other. Strict rules must also be developed for those companies that process credit card transactions, between a sales outlet and their bank, as their files contain information of all the transactions that take place.

Any information held by one party on another party must be responsible and liable for that information in all respects.

Table 3A: (Q4) There's been some discussion about how much liability there should be for bank, retail, and other organizations that keep extensive electronic records on their customers. Which of the following opinions is closest to your own? ROTATE POLES

	%
Organizations that require customers to provide credit card or other personal financial information should be increasingly liable under the law for the impact of successful hacking on their customers	84
No special provisions should be made because the law is adequate and these risks are normal risks that we should all share as a society	15
Don't know or no opinion	1



*Table 3B: (Q5) Should companies whose records systems are
successfully hacked be legally obliged to alert their customers
immediately?*

	%
Definitely	83
Probably	14
Not really	2
Not at all	1

3.0 Methodology

The COMPAS web-survey of CEOs and leaders of small, medium, and large corporations was conducted January 31 – February 2, 2007. Respondents constitute an essentially hand-picked panel with a higher numerical representation of small and medium-sized firms.

Because of the small population of CEOs and business leaders from which the sample was drawn, the study can be considered more accurate than comparably sized general public studies. In studies of the general public, surveys 127 are deemed accurate to within approximate 8.7 percentage points 19 times out of 20. The principal and co-investigator on this study are Conrad Winn, Ph.D. and Tamara Gottlieb.

