Submission to Industry Canada

A Response to the Government of Canada's Digital Economy Strategy Consultation

"Closing the Human Identity Gap"

By Sal Khan
June 29, 2010
skhan@atrust.ca

aTrust Inc.
www.atrust.ca

Relevant Themes

Innovation Using Digital Tecnolologies
Growing the Information Communications Technology Industry

Abstract

Over the past ten years, governments, organizations, and enterprises in Canada and worldwide have seen an increase in consumers choosing to conduct business and access sensitive information online. This swell in online consumer access has resulted in an increased need to provide online, privacy compliant and accurate assurance of the consumer's physical identity and civil identity credentials. The continued use of legacy online authentication systems has led to increasing financial, medical, and data fraud, a growing number of data breeches, sensitive personal information loss, and ever-increasing identity theft. To achieve a significant reduction in online fraud and to prevent identity theft, it is necessary to close the human identity gap, a process which is an integral part of six privacy- enhancing strategic imperatives presented in this submission. If these six strategic imperatives are included in policy and in product requirements, it will result in the development and deployment of technologies and IT systems that can significantly reduce fraud, prevent identity theft, and make privacy, identity, and trust assurance an integral part of eCommerce. The use of privacy-enhancing technologies will create innovation, generate jobs, and enhance Canada's Digital Economy.

Background

The Government of Canada has committed to "launch a digital economy strategy" to drive the adoption of new technology across the economy. This document presents six strategic imperatives, which if adopted into policy and developed into products, will:

- enhance privacy and CyberSecurity
- prevent identity theft,
- result in a significant reduction in online fraud,
- provide greater confidence in the storage of sensitive data stored online (cloud computing)
- build trust and confidence in digital identities,
- enhance eCommerce,
- create innovation, new product development and jobs.

People are the Problem

Most Canadians realize that cybersecurity is compromised, but what most Canadians do not realize is that people are the weakest link in online computer access and internet security. In 2009, researchers at the University of Wisconsin-Madison and IT University in Copenhagen found that until human factors/ergonomics methods are applied to the problem, it isn't likely to go away. Similarly, Sophos, a developer and vendor of security software and hardware, in July 2009, reported that "people are the weakest link in cybersecurity."

People and Identity Theft

While the publicity surrounding the crackdown on identity theft has focused on high-tech schemes to steal computer data over the Internet, a vast majority of identity-theft victims lost sensitive records through non-electronic channels. According to a survey by McMaster University, lost or stolen wallets, credit or debit cards and chequebooks are the most common source of information breach and identity theft. Information stolen by friends, acquaintances, relatives, in-home employees, as well as dishonest business employees is the next major sources of identity theft. Most stolen identities are used to commit financial fraud (offline and online credit/debit card fraud, online bank account fraud) which is disruptive to eCommerce and the digital economy.

An online "human identity gap exists" today.

Digital Identity

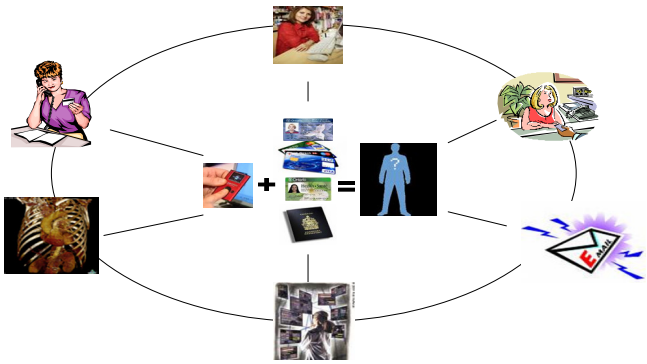

Figure 1 - Identity is Center

To understand what is meant by the "human identity gap," we should first define "digital identity". In simplistic terms, a digital identity is an electronic representation of humans in a digital environment.

A strong digital identity can consist of a human's physical (biometric) identity digitally-bound to his or her identity-proofed civil identity credentials (driver's license, passport, credit card, employer ID) in a *privacy compliant* manner. This process allows digital identity to be used as a central electronic identifier which is essential for trusted eCommerce.

The catchphrase "Identity is Center" was coined by Phil Becker of *Digital ID Magazine* in 2006. In an

article, Mr. Becker wrote: "By using digital identity (including biometric identity) as the key transaction and user identifier, a product or application can offer trusted computing and networking with hsixened security, audited data manageability, and networking flexibilities. If digital identity is treated as the network integrator and organizer, it becomes crucial for distributed or federated tasks, making recipient/sender ID, task compliance/collaboration, and task audit logs and audit trails relatively easy to compile."
To assert the digital identity of a registered consumer seeking access to an online portal, which holds the consumer's sensitive information or bank account, assurances are required about the consumer's identity and his/her civil identity credential(s).

To stop fraud and identity theft *in eCommerce,* ***"Close the Human Identity Gap,"*** *by biometrically authenticating the human and providing assurance about the human's civil identity credentials, as part of the online authentication process.*

CyberAccess – authentication is the weak link

The use of legacy authentication systems has led to an ever increasing amount of financial and medical fraud, data breeches and personal information loss, and an ever increasing amount of identity theft. The 2009 KPMG eCrime Survey reports that user passwords, PKI credentials, one-time-password tokens, and smart cards do not adequately protect sensitive data from sophisticated hackers and organized crime. In August 2009, PandaLabs reported that identity theft via malware was set to skyrocket and password theft, resulting in identity theft from those malware infections, would rise as much as 600 per cent.

Below is a list of methodologies that describe password weaknesses when they are used for online access. To note: passwords are the most commonly-used online access tool today.

- Password crackers get faster and more sophisticated, as well as the computers that run them.
- Hacking tools are now legally sold in stores as Password Recovery tools.
- Physical and logical key loggers can be used without detection.
- Hidden cameras and surveillance cameras are everywhere.
- Algorithms can decrypt passwords based on sound.
- Users have too many logons and passwords and so are often forced to write them down.
- Systems require frequent password renewal and resets forcing users to write them down.
- A third of help desk costs can be attributed to password resets and issuance of new passwords.
- Users are forced to create more complex and longer passwords and have no choice but to write them down.
- Trojans that enter your network via email or Instant Messages have the capability to send logon and password information back to the original creator.

PKI, smart cards, and tokens are definitely one step up from passwords. However, the use of these tools offers no proof that the user seeking access was the authorized user to whom the PKI certificate, smart card, or token was issued. Since 2004, online fraud and identity theft have evolved from simple phishing, to pharming, to man-in-the-middle attacks. Simple phishing can be mitigated with basic fraud detection techniques, two-factor authentication, and user education programs to prevent users from logging into links in email. Pharming redirects users automatically without the end-user clicking on a link. Man-in-the-middle attacks have defeated one time passwords tokens and scratch cards and other forms of shared secrets at large U.S. and European banks. Man-in-the-browser attacks can defeat even smart cards and PKI by modifying the transaction in the browser.

Passwords do not authenticate the human they were issued to or the Service Provider (Relying Party) the human is contacting. PKI certificates, smart cards and one-time-password tokens authenticate only themselves but they do not authenticate the human using them to gain access. The use of these tools has led to online fraud becoming a growing problem for almost all organizations and consumers. Impersonation of an individual using identity information stolen from that individual or from social networking sites is one of the fastest growing crimes today. To prevent identity theft and fraud, it is necessary to verify the physical (biometric) identity of the human as being the authorized user to whom online access was granted. This process authenticates the human and closes the "*human identity gap*," which has become one of the main causes of online fraud and a major drag on the digital economy.

In the event privacy-enabled technologies that are able to comply with the six strategic imperatives (see page 4) are utilized to conduct eCommerce, phishing, pharming, hacking, man-in-the-middle and man-in-the-browser attacks and other such attacks would not be possible.

Identity Theft – a major barrier to deploying a successful digital economy strategy

It has been stated by many experts that Identity Theft is the fastest growing crime on earth. It was indicated in a 2009 consumer Survey by McMaster University that "6.5% of Canadian adults, or almost 1.7 million people, were the victims of some kind of identity theft in 2008[1]". The greater risk of falling victim to identity thieves and stolen identity occurs offline. While headlines may talk of phishing e-mails, key-logging software, and database breaches, more than 80 percent of identity fraud starts offline in the form of misplaced passwords, stolen bank statements, and other paper documents, according to Javelin Strategy & Research. The 2005 Javelin survey[2] reveals that half of the victims of identity-based fraud, who knew where their information had been obtained, stated that the most common source of identity theft was a "lost or stolen wallet, cheque book, or a credit card." Once stolen, the consumer's stolen identity is often used online to commit fraud.

The "2009 Report on Organized Crime in Canada" released on August 7, 2009, by the Criminal Intelligence Service Canada (CISC) outlines the state of organized criminal activity in Canada. In this report, CISC says it expects to see more credit and debit card fraud in the future and that hackers are targeting online sites including online bank accounts and ATMs using various methods such as key logging and malware to steal sensitive information and identities. Finally, the Canadian Council of Better Business Bureaus estimates that identity theft costs the Canadian economy approximately $2.5 billion per year[3].

Whether an online user is accessing a health record, bank account, or making an online purchase, the user's identity can be hacked and stolen. Identity theft results as a consequence of an un-secure online or offline activity. Its consequences are severe but an individual can protect his/her identity by engaging in identity-verified secure online transactions and follow non-repudiable electronic human authenticated transaction confirmation and authorization. As indicated previously in this document, the majority of stolen sensitive information about consumers comes from lost or stolen wallets containing credit and debit cards and it also comes from lost, stolen, or discarded letter mail. However, user ID, passwords and PIN numbers used to access online bank accounts are also stolen online by phishers and hackers, using their software worms and keystroke logging malware. Mainstream password-based authentication is easy to use but most users choose to use the same user ID and passwords to access multiple domains and applications making it easy for hackers to steal their passwords and personal information leading to the loss of their identity and an escalation in fraud.

Below are additional observations from the 2009 McMaster Identity Theft Survey:

1. The 1.7 million victims spent **20** million hours and **$150** million to resolve identity theft and related fraud problems.
2. Most identity fraud involves **financial transactions** as well as social benefits and health-care fraud.
3. Very few of the cases of identity fraud were reported to the police (13%), credit reporting agencies (6%), or PhoneBusters (0.5%).
4. Fully **20%** of consumers eliminated or reduced the amount of online shopping because of concerns about identity theft and fraud,
5. Because of identity theft concerns, 1.5 million Canadians pay $15 per month to credit reporting companies and banks for after the fact Identity Theft Protection.

To grow Canada's digital economy and eCommerce, identity theft prevention should be an imperative which must be eliminated from eCommerce transactions.

Six Strategic Initiatives for Securing eCommerce and enhancing Canada's Digital Economy

Although consumer benefits are well defined, growth in the digital economy raises questions of consumer security and trust. Consumer issues and policy for consumer privacy within Canada's digital economy should have a high priority. Therefore, the Government of Canada should consider developing a policy which includes a strategic initiative to increase consumer confidence in eCommerce. The policy should also embrace a straight-forward means to prevent fraud and identity theft.

The following are *six strategic initiatives* which, if adopted and implemented in products, will help grow consumer confidence in eCommerce, prevent identity theft, and significantly reduce fraud:

---

[1] Source: Measuring Identity Theft in Canada: 200six consumer Survey - Working Paper #23, McMaster eBusiness Research Centre (http://www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-200six-consumer-survey)

[2] Identity Theft Statistics from Javelin: http://money.cnn.com/2009/02/09/news/newsmakers/identity_theft.reut/index.htm

[3] Canadian Identity Theft Statistics from the Canadian Council of Better Business: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00503.html

1. non-repudiable Internet access device authentication, (authenticating the Internet access device which is used to authenticate the human);
2. non-repudiable Service Provider authentication which prevents phishing and man in the middle attacks;
3. privacy compliant, non-repudiable, electronic human authentication (ehAuthentication) that complies with Assurance Levels 1- 4[4] as defined in NIST SP 800-63;
4. non-repudiable, ehAuthenticated (AL1-4) transaction confirmation and transaction authorization,
5. non-repudiable, ehAuthenticated (AL1-4) business transaction identifier as required by (ISO 15944-eBusiness specs),
6. non-repudiable ehAuthenticated (AL1-4) yes/no decision process to accept or reject a transaction.

Identity Theft Prevention – The six strategic imperatives allow consumers to conduct identity-enabled services in a secure and trust-worthy fashion that prevents identity theft. Identity theft prevention is an inherent benefit of the strategic initiatives and an enabler of secure e-Commerce.
To note: current legacy authentication systems can only provide non-repudiable internet access device and service provider authentication (strategic imperatives 1 & 2).

"Our society has become dependent on the Internet for everything from sending email and social networking to shopping and carrying out complex banking and other financial transactions. Yet, for most consumers and even security experts, the Internet is fraught with identity theft, privacy, fraud, and other security risks*." Howard Schmidt US Cyber Security Czar, June 25, 2010.*

By adopting the six strategic imperatives into policy, the Government of Canada will set into motion the use of products that prevent identity theft.

Innovation and jobs

"R&D and technology innovation are crucial to the continued growth and competitiveness of the ICT sector." *Digital Economy Strategy Consultation Document*

"There are technologies that could ensure the protection of privacy in identification and authentication systems. Unfortunately, these technologies are still poorly known and not widely available. There are many reasons for the underdevelopment of these Privacy Enhancing Technologies (PETs) and governments' legal frameworks that do not require or promote the implementation of privacy enhancing technologies, so demand is not felt. Second, the development of these technologies is being held back by various market forces in the software industry. The cost of developing and marketing new products specifically for the purpose of privacy protection seems too high for many in this industry. However, the industry will essentially build whatever is demanded so if PETs become a requirement of government, industry will respond." *Pan-Canadian Strategy for IdM&A Page 32-33 of 180 IATF Final Report.*

"The Task Force spoke to a number of industry experts at the Workshop it hosted in Montreal and at the Privacy and Security Conference in Victoria about the relative unavailability of PETs. All were unanimous in responding that the industry will essentially build whatever the client demands. In other words, the message was that if privacy enhancing technologies are a requirement, government should say so and industry will respond." *Pan-Canadian Strategy for IdM&A Page 33 of 180 IATF Final Report.*

Internet access devices based on the six strategic imperatives can be used directly for network access because they provide strong security for authenticating users and computers and they eliminate the need for less secure password, smart card and one-time-password token-based authentication methods.

In the event the six strategic imperatives are adopted as policy by the Government of Canada, industry will build products and systems that comply with the six strategic imperatives, and in so doing create innovation and jobs.

The Govt of Canada as a model user

"Governments will take the lead and implement a cyber-security strategy to protect Canada's digital infrastructure," and, "By being an early adopter of emerging and next generation technologies (e.g., Green IT and cloud computing models), governments can help drive ICT uptake in the private sector[5]."

The Government of Canada can take its place at the forefront of Canada's proposed new Digital Economy, by taking the lead and making its service delivery application—Canada Access Key (formerly epass/Secure Channel)—the

[4] Assurance Levels (AL) describe the degree of confidence in a user's asserted identity. ALs are usually expressed in numbers and were first documented by the US National Institute of Standards and Technology (NIST) and have since been adopted by many countries including Canada and the European Union.
[5] *Govt. of Canada's Digital Economy Consultation – Improving Canada's Digital Advantage*

innovative cornerstone of its Digital Economy Strategy. To meet objectives related to stopping fraud and preventing identity theft that are found in the Pan Canadian Strategy for Identity Management and Authentication and the Government of Canada's Cyber Authentication Renewal Strategy, the Government of Canada implement into policy the six strategic imperatives presented in this document. The Government of Canada can also take the lead and utilizing privacy enhancing technology compliant products that make use of the six strategic imperatives allowing the Government of Canada to make internal federal applications and consumer-based online initiatives the cornerstones for Canada's new digital economy.

Proposed Federal Cornerstone Applications

1. Canada Access Key (formerly ePass/Secure Channel)
2. myKey (internal federal government online access system)
3. Canadian Health Infoway (policy regarding access to electronic health records)
4. Develop an electronic online voting application

Develop Authentication Policy Guidelines

Levels of Security – We suggest the inclusion of a Level of Security model as part of the Digital Economy Strategy. Levels of security clarify which level of assurance between 1 and 4 is required to protect various levels of sensitive information as part of any online identity transactions. The security level should be based on the sensitivity of the information and risks associated with conducting the online transaction. The different Levels of Assurance is a well-established standard for identity authentication.

Including a formalized concept of standard and interoperable levels of security can provide a good starting point for determining adequate levels of privacy and sensitive information security that must be ensured for secure online transactions. Essentially, a Level of Security would provide guidelines for service providers on the use and maintenance of sensitive information. The strategy should clarify the various level of assurance standard to provide policy, technical, and semantic interoperability for data protection. Without well-understood levels of assurance for protecting sensitive information, it will be much more difficult to create interoperating, trusted relationships online.

For example, does protecting prisoner data stored by Law Enforcement require AL 4 authentication? Similarly, should authentication assurance for the military and Classified Networks also be at AL4. Does access to electronic health records require AL3 assurance? What levels of assurance should apply to transmittal of health information such as digital x-rays and brainscans, access to taxation information, access to SCADA networks, access to online bank accounts and ATMs. What assurance levels are needed for mobile banking/purchasing, and online credit/debit card purchasing?

Conclusion

"We can't go on business as usual, without risking the future of online commerce. This is a watershed year. Everyone you talk to understands that their data aren't safe." Avivah Litan, Gartner Analyst.

The task of building an environment of trust in the digital economy is complex. It involves actions to create an enabling privacy, legal and regulatory environment, and the adoption of codes of practice such as the six strategic imperatives described in this document. Education of businesses, consumers, public servants and service providers is required regarding the availability of secure, privacy compliant and easy to use online access tools. This can only be done if all stakeholders work in partnership, and governments take the lead to and become model users.

A Secure Cyber Access Solution

A first of likely many privacy compliant, secure CyberAccess solutions is now available for use in eCommerce and secure access transactions. This solution complies with, and meets the six strategic imperatives; it closes the human identity gap, prevents identity theft, significantly reduces fraud, and promotes consumer trust and confidence in e-Commerce. As well it can help grow Canada's digital economy as envisioned by the Government of Canada and other stakeholders.