SECURE
SWISS DATA

By David Bruno

It's Time To Make Personal Data Protection A 'National Standard'

SECURE
SWISS DATA

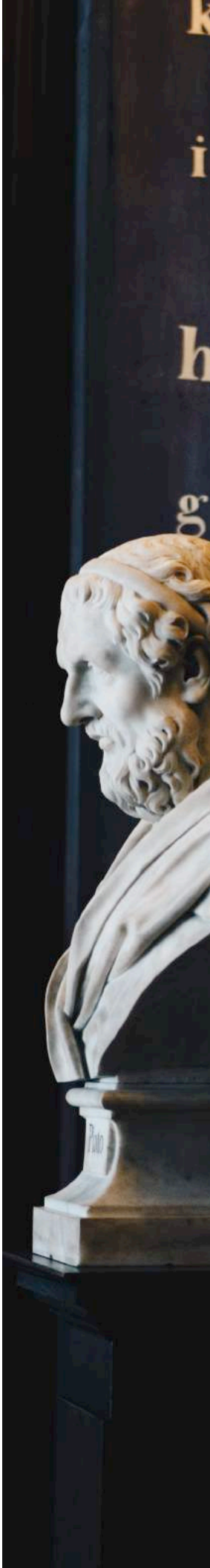
Every day, millions of monetary transactions are intercepted or deployed fraudulently. Credit card details and online banking login information is compromised at a feverish pace, with attackers often selling these details online for less than the price of a dinner.

These attacks are near constant despite the fact that payments are relatively well secured. In September 2006, payment giants MasterCard, American Express, Visa, JCB International and Discover Financial Services congregated to establish the Payment Card Industry Security Standards Council - a body that oversees the protection standards for debit and credit cards issued across the world.

The PCI Data Security Standard (DSS) is now a global benchmark that nearly every merchant, card issuer, financial institution and intermediary needs to comply with. Despite this, payment information falls through the cracks and the global costs were estimated at $22.8 billion in 2016 alone (the costs have since increased).

With this in mind, it should be baffling that personal information and identity data is subject to less scrutiny than payment information. After all, if you credit card is compromised, the bank refunds the stolen funds and a new card is immediately issued. However, you can never change your date of birth, eye color, medical history, Social Insurance Number (SIN) or mother's maiden name.

Critical pieces of personal information like this can be used to steal your identity and used for nefarious purposes. Despite this risk, technology companies and social media platforms treat personal data recklessly, sharing it with third parties and storing it on public forums online where it is nearly impossible to expunge.



SECURE
SWISS DATA

The need for regulations

Controlling and protecting data is a mammoth task that should be the purview of states, which is why the Government of Canada recently stepped in with a pilot program to protect the data of its citizens. The government's proposed CyberSecure Canada program allows organizations to prove their ability to manage and protect data to a certification body approved by the Standards Council of Canada.

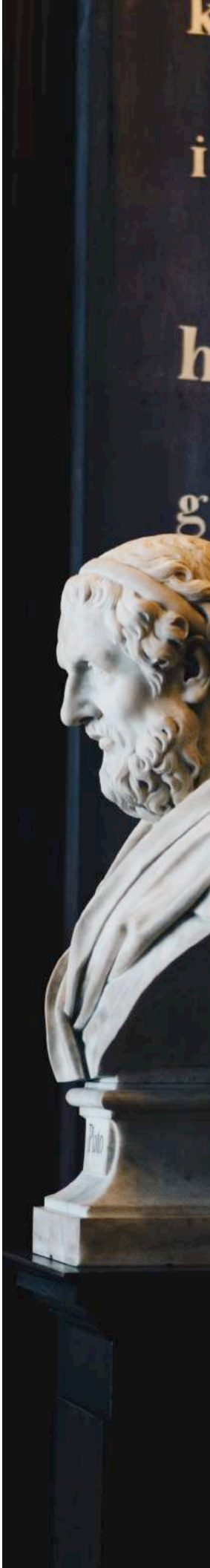
Announced this year by Honourable Bill Morneau, Minister of Finance, the program is still nascent and is being shaped by recommendations from industry veterans and experienced cybersecurity entities like Secure Swiss Data.

Expert recommendations suggest the government's cybersecurity certification program needs to go beyond the intensity of the PCI DSS to be effective in protecting critical data. These recommendations include a tiered system of certification that takes into account not just the size of the business but also the importance of the data it collects.

Better security

PCI DSS compliance is offered on four distinct levels:
Level 1: Merchants processing over 6 million card transactions per year.
Level 2: Merchants processing 1 to 6 million transactions per year.
Level 3: Merchants handling 20,000 to 1 million transactions per year.
Level 4: Merchants handling fewer than 20,000 transactions per year.

However, the standards are designed and implemented by a conglomerate of card-issuers, which means their corporate interests may supersede the interests of average cardholders and citizens.



SECURE
SWISS DATA

The costs of compliance serve as a barrier to entry, which ultimately leads to less protection. Small businesses can expect to spend over $300 per year for PCI-DSS, whereas larger institutions could spends over $70,000 annually.

Finally, the PCI-DSS levels only take into account the volume of transactions to determine security. This is because payments are homogeneous.

However, data is heterogeneous and deserves an added layer of security that accounts for the type of data. Data protection should also be instigated by public institutions rather than corporate conglomerates and should be relatively inexpensive to implement to allow for broader protection.

A hypothetical three level system of Cybersecurity Certification could look something like this:

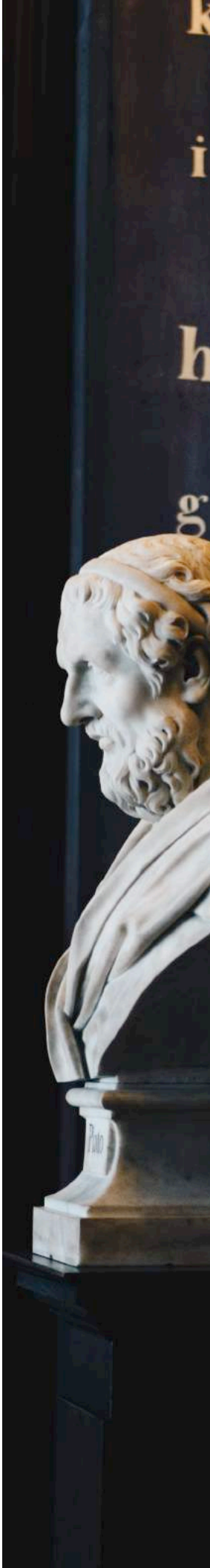
Level 1: Businesses processing less than 1k data points per year. Restricted to minimal data such as name, telephone numbers and email addresses. Not allowed to store data for longer than 3 years. Annual self assessment.

Level 2: Businesses processing less than 500k data points per year. Not allowed critical information such as medical records or SIN numbers. Allowed to store data for up to 5 years. Not allowed to use AI for data collection or use facial recognition software. Annual review by security expert verified by council.

Level 3: Businesses processing more than 1m data points per year. Unrestricted data. May store data indefinitely. Quarterly review by council expert. Mandatory use of approved data security software and IT infrastructure.

About David Bruno

As founder and CEO of a global cyber security firm, David Bruno specialises in anti-fraud and anti-corporate espionage systems for banks and financial institutions worldwide. Through his company, Secure Swiss Data (now SafeSwiss®), he provides financial sector solutions for the digital and interactive e-commerce sectors. For 20 years he has worked to provide security protections to the masses and has invested his own money in a free encrypted email server for the public. He educates on the surveillance of email in general and the importance of encryption, especially for vulnerable populations like refugees.



Going Beyond PCI DSS
For Canada's Data protection

Cybersecurity Certification program could use a multi-level approval system based on the framework for PCI Data Security Standart (DSS) that payments.

The three levels suggested below should go beyond the intensity of the PCI DSS to be sffestive in protecting personal data, which is arguably more important than payment protection.

About PCI DSS

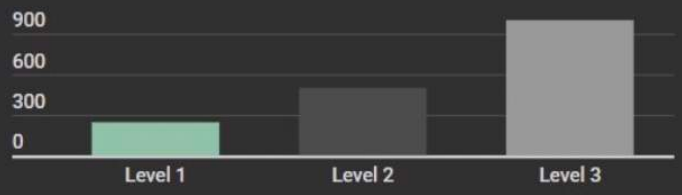
PCI DSS is controlled by a conglomerate of card issuers, is expensive for small and medium-sized business to comply with and is based only on volume of transactions becouse payments are homogeneous.

This system must be modified to suit personal data protections in Canada.

Level		Merchant Transactions (per year)
1		6 million+
2		1m to 6m
3		20,000 to 1m
4		fewer than 20,000

Hypothetical Cybersecurity Certification Program

Transaction Levels



Level 01

Restricted to minimal data such as name, telephone numbers and email addresses. Not allowed to store data for longer than 3 years. Annual self assessment.

Level 02

Not allowed critical information such as medical records or SIN numbers. Allowed to store data for up 5 years. Not allowed to use AI for data collection or use facial recognition software. Annual review expert verified by council.

Level 03

Unrestricted data. May store data indefinitely. Quarterly review by council expert. Mandatory use of approved data security software and IT infrastructure.