Apathy Let Cambridge Analytica Abuse 50 million Facebook Accounts

It was revealed last week that Cambridge Analytica abused personal information from 50 million Facebook accounts in early 2014 to build a system to profile individual American voters for the 2016 presidential election. The goal was to then target the users with personalised political advertisements attacking Hilary Clinton and loving The Donald. It's still not clear whether this was illegal or merely repugnant.

Most people are focussing on the fact that Cambridge Analytica was headed at the time by Steve Bannon, which provides yet another malodorous link to Trump. Facebook's share price is down about 12% but so far there has been no accountability apart from the inevitable class action litigation lawyers circling. What matters the most here is that we are becoming de-sensitized to data breaches like this.

$300M of Etherium permanently lost. Hey, it's just crypto and it wasn't mine, so who cares?

Do you know anyone who lost sleep over 143 million Americans and 100,000 Canadians that were exposed by Equifax's massive data breach.

Every Yahoo account was compromised in 2013, which Yahoo did not figure out until 2017. That was 3 billion accounts. You likely had one of those accounts. Did you complain about it?

Citibank failed to protect the personal data (including birthdates and Social Security numbers) of approximately 146,000 customers who filed for bankruptcy between 2007 and 2011. That's adding insult to injury.

40 million Target customers were exposed in 2013. The remedial cost to Target, not including the class action litigation, was roughly $252M. Did you join the class to get your rightful piece of the settlement?

$81 million stolen from the Bank of Bangladesh by compromising the Swift system in 2016. This was the second time Swift was used as a medium of theft. But hey, that could never happen over here in the civilized world, right?

Look at the lists here and here and here for some of the largest data breaches of all time. How many of these do you remember, or care about?

Even worse, according to the Online Trust Alliance in its terrifying *Cybersecurity and Breach Trends Report* from January of this year, is that 93% of these breaches were self-inflicted and easily preventable. Apathy is our real enemy.

And next up are the assaults from Artificial Intelligence.

AI spans a broad area. A Nest WiFi-enabled thermostat can self-regulate if it feels the sun directly on it rather than air in the home environment – is that 'intelligent' or just good programming? Cruise control on your car? A video game that gets harder the further you go and that learns your favourite moves? Neural networks? Deep learning? The hated robo-advisor? Predictive weather analysis? Smart tokens in the ICO universe?

AI is just a software operating in a hardware environment, but somehow it has gained noble status. Perhaps it's the use of the word "intelligence" that lulls us into thinking that the software is actually alive.

It's not. It's just software, a compendium of zeros and ones that open and close circuits inside chips. Software is vulnerable to coding errors, intentional or negligent. It's vulnerable to breakdowns in its hardware. And it's entirely

vulnerable to malicious third parties for cryptojacking.

Our courts and insurers will have to address who becomes liable when those things go wrong. The worse situation is where software causes death, like earlier this week when a self-driving car killed a woman in Tempe, Arizona. Elaine Herzberg was walking her bicycle when she was hit by a vehicle in autonomous mode going 40 km/h. It doesn't take a crystal ball to see Mr. Herzberg is the first of many such deaths.

Who will carry the financial burden of the error when smart tokens co-ordinate a contract for one billion rolls of toilet paper when the intention was for 100 rolls of paper towel? Is this contract law or negligence? Can you contract out of liability? Medical diagnostic software misses an obvious cause resulting in patient death? Who pays the repair bills when Skynet finally goes live and the Terminator kicks in your door?

Vernor Vinge's 1993 short paper *The Coming Tehnological Singularity* is a marvel of literature that manages to inspire and terrify at the same time. Should something we created actually develop its own intelligence, the pace at which technology would from that point develop would be inconceivable to humans. The human era would be over.

Back to the breaches, both malicious and self-inflicted. Incompetence and thievery have been with humanity for recorded history. The first trojan horse was the serpent surreptitiously attacking the Old Testament God by way of his human creations and an apple. Sadly, we do need various levels of government to help us defend ourselves. This will require some levels of regulation, even if unwanted.

The CryptoCrowd may not like it, but regulation is needed and it's coming. At least there seems to be some regulatory recognition that data is a different world requiring a different set of regulatory parameters. See for example the

British Columbia Securities Commission's 2018 outreach efforts seeking innovation while maintaining confidence in the capital markets.

This apathy is a strange mindset, especially since the business world otherwise takes confidentiality seriously. We sign confidentiality agreements and NDA's. We expect our employees to leave our IP at the office. Securities laws exist to prevent insider trading and to protect the dignity of the market. Larger boards have committees specializing in privacy and data protection. There are few things more valuable to any company than the integrity of its data.

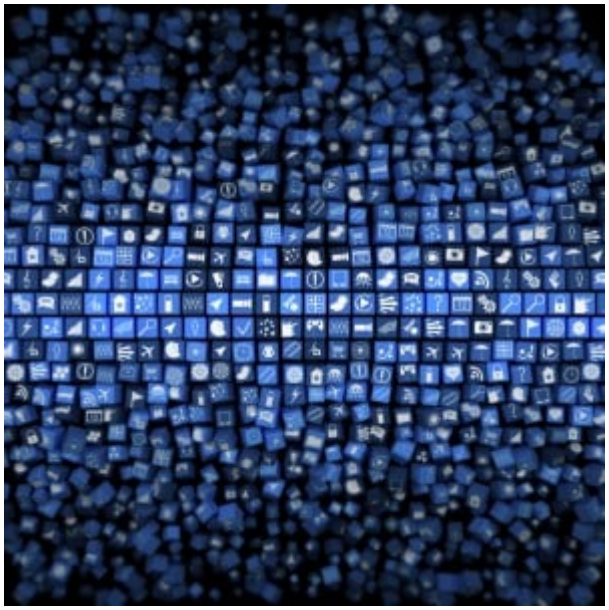
So we should be outraged by these ongoing assaults on us, our data and our companies. We should be in the streets, with torches and pitchforks, demanding that heads roll and attackers be found. Instead, we shrug and say "What can we do? I'm just one helpless person. The government will protect us." That only goes so far.

We have to use what the government gives us. CASL (Canada's AntiSpam Legislation) is a horribly mis-named piece of legislation that has teeth. It codifies an individual's right to control the inbox. It isn't about spam, it's about your digital liberty.

The GDPR is the European Union's approach, and it's a good one. A prior article explaining GDPR is here. Recent recommendations from House of Commons Standing Committee on Access to Information, Privacy and Ethics indicate that Canada will adopt an approach similar to GDPR to give you the tools to protect yourself. So use them.

Ultimately, it's up to you. Be vigilant. Protect your local network. Follow good protocols. Don't be sloppy. And be angry over every breach. Demand accountability. Next time it could be you.

2016: Cybersecurity, Corporate Ebola and CASL



Take the word “risk”. Four letters, such a small word, but those four letters support entire industries, form the basis of global compliance programs and have as many conflicting interpretations as there are words in the thesaurus.

Ask the average person what “risk” means and the answer will be something like, “the chance that something bad might happen”. That’s as good a definition as any for everyday life, but the Risk Management world uses that word in fundamentally different ways.

This definition of risk from investopedia tells the reader everything and at the same time absolutely nothing. It’s a vague idea, requiring context to be properly understood.

Currency risk, execution risk, technology risk, fraud, change in legislation, failure to execute, regulatory investigations, country risk, interest rates, third party risk, liquidity … just some of the predictable risks to a business.

I was speaking at the Global Mining AntiCorruption conference in early October and this topic came up. My point was that I see two kinds of risk: theoretic and functional. Much of what

a compliance department or Risk Manager does is to protect against theoretic visible day-to-day risk. Examples of these are creating process to protect against the Fraud Triangle, buying futures to protect against movement in currencies, having appropriate kinds and levels of insurance, staying current with IFRS to make accurate minimal disclosure, and basic due diligence on third party vendors.

This first level of risk management is absolutely necessary. To a large extent it's "check the box" risk management, supervised largely by regulators with retrospective vision, the International Standards and Accounting Board, and class action lawyers.

Part of Cybersecurity falls in that area.

Cybersecurity was identified by PWC at its 2015 global conference in Monte Carlo as one of the key risks to businesses in 2016. The cybersecurity insurance market is estimated to be worth USD$7.5B by 2020. IIROC, the self-regulatory body for Canada's brokerage firms, takes this so seriously that in December, 2015 it issued a standalone Cybersecurity Best Practices Policy aimed at small and medium sized firms.

There will always be hackers trying to breach the company's castle walls. It's a constantly evolving arms race between the people who own the data and the people who want it.

Some of those battles might be lost from time to time, but one part of cybersecurity where no company should ever lose is in its CASL compliance.

We have been banging on the CASL drum for about two years and will continue to raise the alarm. A failure to be in compliance has the potential to wipe out your company. It is that serious. See a recent article here that outlines why CASL should be seen as corporate ebola.

A quick recap of CASL's basic tenet: before you send any electronic message (email, BBM, proximity based marketing) to an account (email, phone, Bluetooth), you MUST have that account holder's prior consent. You cannot message to ask for consent to send a message – you must already have consent to send the message. The onus is on you as the sender to prove you had that prior consent.

There are other rules, limits and exceptions in this Canada-wide statute, but that's the key principle to keep in mind.

Currently, the only consequence of a failure to comply with CASL is a prosecution by the Canadian Radio-television Telecommunications Commission (CRTC) and possible fines. The maximum penalty for a violation is $1,000,000 for an individual and $10,000,000 for a corporation, in addition to the legal costs, the cost of distraction and the public relations damage.

I've spoken with dozens of companies that have said, "Sure, but the CRTC will never prosecute us. We're too small / invisible / almost in compliance." All of that is probably true. With over 99% of companies NOT being in CASL compliance, the odds of a negative consequence to being in breach is minimal.

The problem is, that will change in July of 2017. That's when the courts begin to share jurisdiction over CASL breaches. You and your company can then be sued for CASL breaches. Yes, in court, and supportable by class action litigation. And the onus will be on you as the sender to prove you were in compliance – the plaintiffs will not have to prove you weren't in compliance.

That's as scary as it sounds. And it is the law of Canada.

The law applies to any email received in Canada. So imagine a Florida-based company with a sales subsidiary in Calgary, sending emails that are offside CASL. Even an articling

student can see the path is to bring class action litigation against the Calgary sub, and allege the Florida directors were negligent in failing to ensure good Risk Management protocols were in place. Bang! A breach of CASL in Canada comes home to Florida.

Anyone who emails for business reasons into Canada is at risk, regardless of where your home office or servers are located. CASL can follow you extra-jurisdictionally.

This is the new reality, a simple decision to make, based on obvious Risk Management principles. The massive risk clearly exists, so welcome to 2016: get into CASL compliance now and avoid being sued in 2017.

Make sure CASL compliance appears as a line item in this year’s budget. If it’s not there, ask your Risk Management team why not.