Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

Privacy Management: In Enterprise we Trust

Keynote Presentation to the CISO Executive Summit June 4, 2014

Elizabeth Denham
Information and Privacy Commissioner for B.C.

It is a pleasure to be here. When I was here two years ago to deliver an opening address for the first-ever Vancouver CISO summit, I was so impressed by the smart questions, energy, and engagement. There was a buzz in the room! That can be pretty tough to do – especially at 8 in the morning! But we had it – and it was a fantastic event.

Which is why in 2014 I stepped forward to be a member of the governing body. You will see there are several different sessions that have a privacy and data protection theme. I may have had a little something to do with that.

Kudos to the conference co-chairs, fellow members of the governing body, and to Scott Pond and his team at Evanta for pulling together such a great agenda. And thanks to all of you for taking time out of your busy schedules to be here. I'm looking forward to your questions, and to speaking with you over the course of today.

I'm going to talk about three things in my speech today.

First, I'm going to talk about why privacy matters. Second, I'm going to talk about why privacy should matter to you as a CISO. And third, I'm going to talk about a tool you can use to implement across-the-board privacy controls for your company or your agency.

When I first started to prepare for this speech, I looked back on the issues in privacy and security making headlines in the past year. And it gave me whiplash. We had a hugely busy year!

Some of you might think of 2013 as the "year of the data breach" – when hackers stole credit card data and personal information from 110 million customers at Target. This breach has had a serious impact on profits and both the Chief Executive Officer and Chief Information Officer resigned.

And just when we thought breaches couldn't get any bigger – a couple of weeks ago, EBay stepped forward to reveal that hackers raided its network three months ago, accessing some 145 million user records of which they copied "a large part".

The records contained passwords as well as email addresses, birth dates, mailing addresses and other personal information. It is one of the biggest data breaches in history, based on the number of accounts compromised. And the data breach problem is intensifying.

A recent survey from IBM Canada found that Canadian businesses have experienced a 38% increase in significant data breaches in the past year. This is a very real and a very serious problem. I think if you talk to the average person on the street, they would say: "We need to do something about this."

Which is why in late May – in the context of the hearings of a legislative committee reviewing PIPA, I called for government to amend BC's private sector privacy law to include mandatory breach notification. This amendment would require organizations to notify both my office and affected individuals in the event of a privacy breach that creates a real risk of significant harm.

Mandatory reporting is an incentive for companies to focus on privacy and security, and it would level the playing field for organizations who already have to report in other jurisdictions, like Alberta, or the 47 out of 50 states in the U.S. that have mandatory security breach notification in law. It also needs to be flexible, and the reporting regime needs to reflect the business community in B.C., which is made up of a lot of small businesses and microbusinesses, as well as a lot of start-ups. We are also studying the need for mandatory breach reporting in the public sector. More about this in the months to come.

2013 was also the year of surveillance. Edward Snowden's revelations shook the public trust in national security agencies. Nearly a year after the NSA whistleblower became a household name; we still see media stories breaking new ground on the topic of secret surveillance.

I think there is much more to come on this file and Commissioners across Canada have called for a parliamentary and a public debate on the surveillance activities in Canada. We will hear from representatives from both CSIS and CSEC on the issue of oversight of our national security agencies in the following session.

For these reasons and more, dictionary.com chose "privacy" for their word of the year in 2013. Nearly everywhere we looked, journalists, citizens and civil society raised questions about privacy and security of personal data. As Privacy Commissioner, I think that's a very good thing.

Despite the circumstances that brought these stories to the fore, the fact they are making headlines than ever. We saw this recently in the editorials and news stories criticizing the PMs nomination of the next Privacy Commissioner of Canada, Monsieur Therrien. And it proves that despite sweeping changes in technology and an explosion of data gathering privacy is still a deeply held value.

We all have the right as individuals to keep a private life, separate and apart from our public life. Our right to draw that line, and control that line, is essential in a democratic society built upon the values of freedom of association, and freedom of expression.

Our economy also depends on privacy and data security. Imagine going to a credit union for a loan, to a lawyer to draw up a will, or to a financial planner for advice without any guarantee the information you provided would be respected and kept secure.

Privacy matters because the costs of data breaches, identity theft and other misuse of our personal information are real, substantial and mounting. These losses harm us, but they also hurt your company's bottom line.

Case in point: Each year, the Ponemon Institute publishes a global survey of various industry sectors to quantify the cost of a data breach. For 2013, the global average cost of a data breach was $145 per record. The number of compromised records in the average data breach was just over 23,000. Do the math and you'll see that the average cost paid per company, per breach, was $3.5 million dollars. And that's just the direct cost. The Institute also measured the cost of lost business. By way of example, our neighbours to the south saw an average of $3.3 million dollars in lost business costs, the highest among all countries surveyed.

Interestingly, the study found that CISOs can reduce the direct costs of a data spill. Having a CISO with enterprise-wide responsibility, an incident response plan and a

strong security posture could bring the per-capita cost down to $33.50 per compromised record or a 75% reduction of the average per-record direct cost. If that isn't enough to convince you that investing in privacy and security is important – consider that privacy is an essential and urgent concern to your customers.

A 2012 study of consumer attitudes in Canada found that 72% are concerned about the erosion of their privacy. Privacy concerns were more important than climate change and terrorism, and were second only to a second global economic crisis. Keep in mind these stats were gathered before Edward Snowden. I expect privacy concerns rank even higher today. To their credit, Canadian businesses recognize this growing concern about privacy. 63% of businesses surveyed identified strong privacy practices to be a significant competitive advantage.

These companies recognize the opportunity to build trust and confidence thorough comprehensive privacy practices. The million dollar question is – are you prepared to seize the opportunity to demonstrate your strategic value, invest in strong privacy and security controls and meet the demands of your customers?

As data becomes more mobile, is stored in exponentially larger amounts, and flows between organizations and across borders – you have increased responsibilities and increased challenges as the gatekeepers of your company's data. Your job is to look out for data security above all else – but you also can't be seen to be the Department of "No", when it comes to new technologies and new opportunities. If you do, employees or business units might just find a way to sidestep your policies and directives – taking matters, and personal data, into their own hands – with potentially disastrous results.

Your company counts on you to chart the right course – to say yes to new tools and toys in a way that also ensures privacy and security is locked in. What if I told you there was a tool you could use to reduce the risk and build privacy into your business? This tool was created by Privacy Commissioners across Canada tailored expressly for businesses to implement comprehensive privacy management in the private sector.

The document is called "Getting Accountability Right with a Privacy Management Program". It is a joint product of the Office of the federal Privacy Commissioner, and the Offices of the Commissioners of British Columbia and Alberta. Those of you who are in the public sector will be pleased to know that here in B.C. we have developed an accountability document specifically for public bodies subject to the *Freedom of Information and Protection of Privacy Act*.

While the legislative framework is different, both programs emphasize the same, scalable building-block model starting with an organizational commitment to privacy—that means tone from the top, and a genuine commitment to invest in privacy that is communicated by the head of the company.

The foundation includes creating a Chief Privacy Officer role. This person should have a voice at the executive table and should be empowered to lead the privacy agenda for the business. Once this foundation is laid, program controls are necessary, followed by ongoing assessment and revision—this is critical in light of changing threats and risks.

The key is that privacy and data protection is not a one-time investment, or a one-off activity. It is an ongoing, evergreen process that must be done in a holistic way. You can't just say, 'Oh yeah, privacy – we did that in 2004', that doesn't work. Privacy Commissioners across Canada are using this framework in enforcement work to measure an organization's compliance with the law. This is part of a broader regulatory shift away from focusing in on specific incidents – such as whether your business had reasonable safeguards in place in light of a data breach – towards a comprehensive assessment of your overall privacy and security set-up. We've put companies on notice that they must stand ready to demonstrate compliance with the law and what we expect to see in place!

Here in BC, I've applied an accountability lens to several systemic investigations including BC Hydro smart meters, the use of facial recognition technology by ICBC and the use of automated licence plate recognition by the Victoria Police Department. In those investigations we took a more holistic view of these organization's overall privacy program – whether they had the capacity to comply with their obligations, and included specific recommendations to improve their security policies and practices.

The accountability framework has been around for a couple of years now. In that time we've focused heavily on education and outreach. I've been on the road promoting the guidance with a lot of different audiences. And we are starting to see results! I would like to share with you some shining examples of how it can be done. I also want to show you that organizations of varying sizes and business models have successfully implemented privacy management using the tools I've described today.

What these organizations have in common is they are walking the talk and that an investment in privacy is making a meaningful difference. In the wake of a data breach at the University of Victoria affecting payroll data of more than 12,000 employees, the senior administration made the decision to make a lasting investment in privacy, data security and records management.

The project is led by a coordinating committee, appointed by the University President, who oversees the development of integrated work plans for these three areas in consultation with the CPO, the Archivist and the CIO. Clearly there is buy-in and active involvement from the top. They started with the monumental task of assessing the confidential record holdings in nearly 200 administrative offices. They reviewed the results of each unit, giving them specific feedback to improve privacy and security practices.

Some of the progress they've made includes: a campus-wide antivirus and encryption service, and set out mobile device policies to increase the security of personal information; an investment in ongoing staff training and establishing a matrix that determines which projects need a privacy impact assessment. With more than 4,600 faculty and staff and 170 administrative offices this was a major undertaking. The university reports out on its progress in an annual report dedicated to privacy and security issues.

In 2013, Elections BC – an office of the legislature with about 40 staff – decided to make a lasting investment in privacy. Developing a formalized privacy management framework was a key priority for the 2013/14 fiscal year. The decision to make privacy a priority was made by the executive team, who champion the cause and empower their Chief Privacy Officer to lead the implementation across the organization.

They started by reviewing their inventory of personal data. They hired an expert to help them with this work, and following from this initial investment identified more than 100 areas for improvement in their current practices, which they are currently working through. They've also experienced success in that staff who have been trained to identify privacy issues in one context, are applying those skills in others – including when they're looking at new projects, new systems or technologies. They're seeing privacy in full colour.

The Law Society of BC is a regulatory organization with 200 employees overseeing the professional conduct of more than 10,000 lawyers in B.C. In 2012, the Law Society conducted a privacy assessment of the entire organization to see how well it was protecting personal information and identify areas needing improvement. Since the assessment, the Law Society has made a number of changes to enhance physical and technical security. A Privacy Compliance Officer (PCO) position was created and filled in January 2014. In April, the Law Society's Privacy and Information Technology policies were updated. To ensure all employees were aware of the new policies, mandatory privacy training sessions were completed.

These are but a few examples of organizations that have made privacy and security a part of their DNA. It is my hope that you will follow their good example and lead the charge in your organizations for all of the reasons I've outlined here today.

In closing, I want to say that while CISOs are critical to the privacy game – at the end of the day, privacy is a team sport including your executive, legal counsel, records management, communications and operational teams.

This teamwork is also needed in the broader community. We need a lasting commitment in the public, private sector, industry, government and regulators to promote privacy and security in the years to come.

If your team plays the privacy game, and does it well, you stand to attract and retain a growing number of discerning customers concerned about the fate of their data – giving you a huge competitive advantage in an increasingly crowded marketplace.

I welcome any questions that you have.