Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

“Privacy, Security, Accountability: Best Practices for CISOs”

Elizabeth Denham
Information and Privacy Commissioner for B.C.

Keynote Presentation to the

CISO Executive Summit
June 12, 2012––Vancouver, BC

Thank you for that kind introduction.

And thank you to the Evanta board of directors for the invitation to speak.

It’s a pleasure to be here and to be a part of this inaugural CISO conference. What a great opportunity to connect, collaborate, share solutions and best practices with your peers.

It’s also a great opportunity for me… because I have a captive audience… and a microphone… and a podium…

Just kidding! I’m excited to be here because I get to talk about some of the work we have been doing, and to share some my insights with you.

It's been almost two years since I was appointed Information and Privacy Commissioner for B.C.

Hitting the one-third mark in my term is exciting because I'm seeing how the ideas we put in motion shortly after my appointment are starting to bear fruit—both in improved service to the public, and moving the yardstick for access and privacy rights.

Allow me to share just a few examples of the progress we've made on some of our key priorities.

One of the first changes I made when I took office was to reorganize staff resources, to allow us to do more proactive work on the broader policy issues affecting information rights.

Up until that point… if there was a privacy breach, our office could investigate. If personal information was being misused or mishandled, we could look into it and order changes.

While this approach helps individual complainants, and can provide retrofits and program changes ….it only does so after the fact.

I wanted to increase the capacity of our office to be more forward-looking, and better able to tackle some of the bigger privacy risks on the horizon.

So, I reorganized our staff into two teams – a group to continue working with the complaints and inquiries coming through our front door… and a policy and technology group whose focus is systemic investigations and proactive reviews.

In the past two years we have closed 2,377 files and, in fact, we completed our investigations 6 weeks faster on average. In addition, since 2011 our policy team has published four systemic investigation reports, and initiated two more.

We've examined the privacy and security controls in BC Hydro's smart metering program, ICBC's use of facial recognition technology software, and an online gaming platform at BC Lotteries.

These investigations go beyond the surface issues. They provide guidance to public and private sector organizations about how to strengthen privacy programs overall.

Another area that I've been very focused on is building our office's capacity to address the impact of new and emerging technologies on privacy—everything from social media and mobile technology to the new data-sharing and e-health initiatives underway by government.

Our office is very much live to the privacy and security issues inherent in these technologies. And we know that citizens, consumers, and companies are looking to us for guidance on how we ensure that privacy and technology are complementary values, not competing values.

To address this challenge and to build our capacity to work through some of these issues, I hired a technical security expert, Angela Swan, who has been an invaluable addition to our team.

Angela is a CISSP and is also a CISM.

We now have someone in-house to consult with as we increasingly deal with privacy issues related to encryption, cloud computing, location based systems, and other technologies in our day to day work.

We've also published new guidance to give the public bodies and businesses some best practices to follow as they dive into these technologies. For example, we published guidelines for employers on conducting social media background checks, an interactive security check- list for businesses, and cloud computing guidelines for public bodies.

Guidance on cloud computing for the private sector is coming online very soon – check our website for more details later this week.

My third key priority since taking office is to enhance our public education and outreach.

For the first time, we have a Manager of Communications and Public Education, a position dedicated to increasing our reach and informing citizens and consumers about their privacy rights.

Last year we increased our speaking engagements by 80%, delivering 90 presentations to public and professional audiences, such as this one.

We increased the numbers of op-eds and open letters. Most recently you may have seen a series of letters I wrote to the Legislative Assembly regarding Bills that I believe undermine British Columbians access and privacy rights. I've also joined my federal and provincial colleagues to express my deep concern about a federal bill, C-30, the government's on-line surveillance legislation, a.k.a. "lawful access".

Advocates and commissioners were successful in at least stalling this bill, and we are hoping that parliamentarians will debate and reconsider its sweeping powers for law enforcement to access our personal communications without judicial oversight.

Back to British Columbia.

The media is covering our work and commentary; interviews are up by 30% this year.

These numbers tell me that we are doing a better job of engaging the public and staying current with what is happening outside our office walls.

We're looking to grow our private sector privacy education, an area where we think there is a real lack of awareness – both among businesses and consumers. And we're working on some strategies to address this gap and promote awareness and compliance.

As you can imagine, with all of these new initiatives, it has been CRAZY busy in our office. We are a very lean operation—with a total of 33 staff—responsible for independent oversight of the practices of 2,900 public bodies and 300,000 private sector organizations in the Province.

As Commissioner, I have investigative and audit powers, the mandate to make public comments on services or initiatives that affect information rights. I can make orders that are legal and binding on an organization.

I like to think of us as the "little office that could".

I am incredibly proud of the work we've accomplished in two short years.

But today, I'm here today to talk about accountability… and the need for Canadian business to start walking the talk and demonstrate sound privacy management practices.

We've partnered with Privacy Commissioners across Canada to create a tool that will help you to address some of the key privacy and security issues facing your business and help you to comply with Canada's privacy laws.

It is also a tool that can help you address some of the challenges you face as a CISO.

I don't think it will come as a surprise to you that many people think of the CISO as the CNO…

…the Chief No Officer.

Once upon a time, I was a Chief Privacy Officer and people expected me to be the CNO. They were so used to privacy getting in the way of moving forward on new initiatives.

There is a misperception out there that CSOs, CISOs and CPOs are roadblocks, rather than enablers of innovation.

When your employees think about building shiny new systems…

When they dream up new ways to share and store information…

When they see the business opportunities inherent in new technologies…

Many of them come to you with these ideas…. expecting to be shut down.

No, you can't store client information in the cloud!

No, you can't use your tablet in the office!

No, you can't create a website to give customers online access to their files!

The spectre of 'No' can be enough for some employees to take matters into their own hands, to create workarounds… or to implement changes without consulting IT or the Security Officer, a move that could have consequences for the company as a whole.

The challenge for those of you in this room… is getting from No… to Yes.

Yes, we can build this, and here is how you do it by building in privacy and security.

BUT…. and there is a but….

To get to YES, you need a strong business regime for managing personal information.

The solution is to create a privacy management program to address these issues…to lay the groundwork…before systems are built. Privacy BEFORE Design.

A privacy management program is a constellation of policies, controls and best practices that work together to protect and secure personal information across the board.

It underpins all systems that touch personal data.

A privacy management program will not only get you from NO to YES, but it can also help you demonstrate and enhance your value to your organization, and help others to see that you are a leader, an enabler and an innovator, not a roadblock.

So: What is privacy management? What does it have to do with accountability? And why are Canada's Privacy Commissioners leading the charge?

In brief, Canada has had private sector privacy laws in place for about a dozen years now. First, the province of Quebec passed a law governing privacy practices in the commercial sector, then, PIPEDA was passed by the federal government. Alberta and British Columbia followed suit with their own legislation in 2004.

At the heart of that legislative framework is the principle of accountability. The idea that organizations are ethically and legally responsible for the personal information they collect.

Now, it has never been a challenge to get organizations to say that they are accountable. The challenge has always been to get organizations to prove it in practice.

Consider the following statistics, collected by the federal Privacy Commissioner in 2011.

77% of Canadian businesses say that protecting privacy is extremely important, or very important.

Fantastic!

39% of those companies say that they see protecting privacy as a competitive advantage.

Even better!

But… there is a disconnect.

While 77% Canadian businesses say privacy is important or very important…only 62% have a privacy policy.

Two-thirds of Canadian businesses **do not** have procedures for assessing privacy risks.

Two-thirds **do not** have policies to address privacy breaches.

43% **do not** have a person designated as responsible for privacy.

And nearly 70% **do not** have staff training in place on privacy issues or risks.

The survey also found that Canadian companies who say that privacy is important … are aware of their privacy obligations … but also perceive compliance to be difficult.

So…there is a discrepancy between companies that say they care about privacy…and those who actually “walk the talk”.

As Commissioners, we have seen this play out again and again, in the course of our investigations.

There are some sweet spots – certainly some financial services companies, telecommunications providers and health services have adopted very sophisticated information governance programs.

But Canadian companies across the board, particularly professional services companies, and many retail companies have not even begun to put the basic controls in place.

In light of this experience as Commissioners, we wanted to create a resource that would help businesses understand privacy management, AND that would also give the businesses tools to comply with the law.

The tool is called “**Getting Accountability Right with a Privacy Management Program**”, and it is your roadmap to sound data governance. The paper is practical, workable and scalable and will help your business demonstrate accountability and better protect personal information.

The paper takes a “building block approach” to privacy management. By implementing these building blocks, you can demonstrate to customers, clients and regulators that you are committed to privacy and accountability, enhancing your reputation and building trust in those relationships.

This is a sea change in that Commissioners are moving beyond asking just for technical details.

In the wake of a complaint, investigation or audit of a business, we will ask for evidence of the privacy management program in place, and, in significant cases, we will be assessing that program as part of our investigation or audit. The whole is greater than the sum of the parts.

The building blocks begin with **organizational commitment** to develop a privacy-respectful culture.

This has to start from the very top—with buy-in from senior management. Only then, can responsibility be truly delegated to a Privacy Lead, perhaps supported by an office or delegation with clear roles and responsibilities.

Next are the **program controls**, starting with a documented inventory of what personal information you hold, where it is held, its level of sensitivity and the purposes for which it is being collected, used and disclosed.

Once the building blocks are established, a business has to have a mechanism in place to monitor, assess and improve its program.

Ongoing assessment and revision is critical in light of changing threats and risk—you must be updating and fine tuning the controls to ensure they are relevant, adaptive and effective.

What’s in it for businesses that adopt privacy management in practice?

The document is a roadmap to sound data governance. It is ready for you to adopt and implement, step by step.

The framework is inter-operable, which means there will be certainty for business and consistency in Commissioner’s expectations across the country.

It gives guidance to pathfinder companies. Global companies will have an enterprise risk program in place. But regional companies may not need to build such sophisticated programs. The guidance is intended to be scaled to the size and needs of the organization.

AND good privacy management will have evidentiary value in an investigative proceeding by Canada’s privacy Commissioners.

Thinking back to those statistics I mentioned earlier… adopting a comprehensive program will help your company hit all the bases for an accountable organization.

If an organization has these elements in place, there is a trusted environment—and Commissioners and customers will have confidence that you comply with the law.

A strong privacy management program includes a thorough review and audit of all systems and networks that manage and store customer and employee data. It also includes developing contingency plans in the event of an incident or data breach. In other words, it can help you to do your job more effectively—and has the potential to ensure those standards are propagated across the whole organization—getting everyone, not just IT, thinking about security and privacy.

The bottom line: Privacy management is not a one-time thing, or a one-off. It takes a fundamental commitment, supported by a strong team that includes CISOs. That team must be committed to creating a “culture of privacy” rather than the “paperwork of privacy.”

An investment in privacy up front is a far better bet than cleaning up the mess after a catastrophic data breach, a costly way to erode your brand.

Some of you in the audience might be thinking, sure—easy for you to say from up there … but how can I actually apply privacy management in my company? Where do I start?

First things first. Build a culture of accountability / commitment along with other key decision makers in your organization.

Designate a privacy officer – IT's a legal requirement. Support their work across the company to build a robust privacy framework.

Sidebar: (Interesting to read that LinkedIn, which confirmed that 6.5 million hashed passwords were compromised, has no one specifically tasked with assuring the privacy and security of its data and systems.)

Once you have a privacy lead—[and you may be the person wearing this hat!] Make sure you are at the table when decisions about new products, services and business models are made.

Don't have a privacy policy? Start the work to create one.

Once you have these basics in place, then move to the next building block in the framework.

Document what personal information you hold and where it is held. Is it in the hands of service providers? You are still accountable for this data at the end of the day.

Create contingency plans in the case of a privacy breach. You'll need a command and control approach to properly manage a breach. Best to be clear ahead of time what roles you will play and who is calling the shots.

I would also encourage you to do some spot audits to test how well your policies are being implemented. For example, if your company has a policy that all personal information stored on mobile devices—like laptops, tablets and thumb drives—must be encrypted—how many employees are actually following through on that policy?

By the way, when it comes to storing personal information on mobile devices, encryption is the minimum standard. Password protection is not enough. The University of Victoria recently learned this lesson the hard way, when an unencrypted disc of 12,000 employees' data was stolen from the administration building.

Maybe you are particularly proud of the privacy and security measures you implemented for a recent project.

Why not try to animate those principles and bring them to bear in an overall privacy management program, so that all projects can benefit from the proactive and thoughtful privacy and security considerations at play in those new systems.

These are just a few examples of how the accountability tool can be made to work for your company—even if you think you take privacy and security seriously.

The tool is available for download on our website; there is a two-page primer as well as the full document with guidance.

***

Now, to this point I've done all the talking. But I believe that as a regulator, listening is just as important, if not more important, than talking.

I will be here for a portion of the day, to take in the conference, and to listen in on some of the discussions.

I look forward to speaking with some of you, and hearing from you about what's on your mind when it comes to access and privacy.

In the meantime, I am happy to answer any questions you may have.