Protecting privacy. Promoting transparency.

CHECK AGAINST DELIVERY

HOUSE OF CARDS: PRIVACY, SECURITY AND INFORMATION GOVERNANCE IN A DIGITAL SOCIETY

SPEECH TO THE

EVANTA CIO EXECUTIVE SUMMIT

JUNE 2, 2015

ELIZABETH DENHAM
INFORMATION AND PRIVACY COMMISSIONER FOR BC

Thank you ,and thanks also to the governing body for the invitation to speak.

This is my third Evanta event, but my first time speaking exclusively to CIOs. You have been on my radar as a target audience for a while now, so I am happy to be here!

And what better time for the Privacy Commissioner to be bending the ear of executive leads for all things information security…than in the wake of my recent investigation into the District of Saanich's use of employee monitoring software.

I expect that some of you will have read my report, but for those who haven't… my speech this morning will give you the Cole's Notes.

There are some valuable lessons there for both public agencies and private sector CIOs.

But before I get to the Saanich report… I want to talk about why CIOs are on my radar and why it's important for us to get together and talk about privacy and data security.

CIOs + Privacy: Common Challenges/Opportunities

Rapid advances in technology have moved information and data to the forefront of the modern enterprise.

Government and businesses can quantify, collect, share, analyze and MONETIZE data like never before.

While information has always held tremendous value for organizations, the digital age has made the PROMISE and POTENTIAL of information and data more important than ever before.

In this context, the role of the CIO has become more prominent and important.

The CIO is no longer siloed away. You are a key player at the executive table. Your insights aren't just limited to how to keep key systems running -- your expertise effectively advances the company's strategic goals.

Your role is also more complex than it was 10 or even 5 years ago.

Today, CIOs must also have knowledge of -- and bridge the divide between -- market research, mobile applications, big data sources, and cybersecurity in order to succeed.

You are under pressure to leverage new tools to promote innovation, drive sales, and find new and better ways of working.

You are expected to use big data analytics to find the needle in the haystack… to turn the breadcrumbs of customer data into valuable – and profitable – insights.

You must address the power shift to users – mobile, BYOD and cloud-computing…and you must anticipate AND address evolving cybersecurity threats.

At the same time, CIOs are faced with a sea change in citizen and consumer expectations.

Individuals are demanding control over their personal information, transparency about how their data is handled, and security controls to protect it.

Today, when massive data breaches happen, and the torches and pitchforks come out, they come to the CIO for answers.

It is worth pointing out that in the fallout of the Target breach… the first head to roll was that of the CIO.

These are all important drivers in the work that you do.

But I am here to tell you that you are not alone.

What keeps you up at night… is what keeps me up at night!

The privacy world has changed dramatically, too.

Back in 2007, when I was Assistant Privacy Commissioner of Canada – I remember one day, we were perplexed by a meeting request that had just come in. The company was Salesforce. And they wanted to talk to us about the privacy implications of a new service called….cloud computing. We had to scramble to figure out what this was all about to appear to be knowledgeable regulators. And that wasn't so very long ago!

Fast forward to today and IM/IT issues and the technical aspects of privacy enforcement are front-and-centre in our work.

Privacy regulators are grappling with similar challenges – from data governance and data flows among and between mobile devices, to getting the balance right in new systems to make sure information is secure against unauthorized use and disclosure, but also available for business purposes.

I would also suggest that our respective roles – CIOs and Privacy Commissioners – are more important than ever.

We live in a world where neither information security nor privacy is optional. You have a responsibility to secure networks and protect data. Privacy is a legal obligation. And privacy is a team sport, one in which CIOs and information managers are key players.

British Columbians count on us BOTH to get privacy and security right… and to strike the right balance.

Privacy and Security

Before we go any further, a word about privacy and data security and how they work together.

Privacy is a quasi-constitutional right. It is the right to be let alone, the right to keep certain thoughts, communications, or actions private. It is central to our sense of self, and it is an instrumental personal freedom. Protecting privacy is also a legal obligation for governments and businesses.

You can have security without privacy, but you can't have privacy without data security.

Data Security is the implementation of necessary controls to prevent against loss, theft or compromise. In a digital society, we all expect governments and businesses to secure networked systems against known vulnerabilities. Threats to an agency's information assets from both internal and external sources have been well-documented. And reasonable security controls to protect personal information are also a requirement under privacy law.

The balance between privacy and security is not a one-size-fits-all proposition. It will always be settled in context, on a case-by-case basis. Where privacy and security come into tension, we must weigh the risks and benefits, carefully checking the proportionality of the privacy intrusion, against the demonstrated need.

When the balance is right – privacy and security co-exist. The house of cards stands stronger, benefiting those whose sensitive personal information is housed inside.

And trust and confidence is built among citizens, shareholders and regulators.

But what does it look like when the balance is NOT right? The house of cards falls. Trust is lost. And there's usually a big mess to clean up afterwards.

Saanich Report

Let me tell you the story of what happened in Saanich.

In January of this year, a couple of months post-election, Mayor Richard Atwell called a press conference, where he alleged—among other things—that he was being spied on and that there was software installed on his computer without his consent, to monitor his activity.

In response, Saanich Council released background information on the software that the District had selected – Spector 360 – and their rationale for doing so. They also made a very troubling statement: That employees have no reasonable right to privacy in the workplace, they said.

As Commissioner, I could not let that statement go unchallenged. Nor could I ignore the growing number of unanswered questions about the use of the software by the District.

So I initiated an investigation—on my own motion—to examine whether the use of this software by the District complied with the *Freedom of Information and Protection of Privacy Act*. And to reinforce the fact that employees do have privacy rights in the workplace.

From mid-January until the end of March, we took a deep look at the “what” of the software—how it operated, what it collected, and how it was secured—as well as the why. We asked the District to explain their legal authority to collect personal employee information using this software tool. We also looked at the when and pieced together a timeline, from the decision point to procure the software... all the way up to installation and the Mayor’s press conference.

We uncovered some interesting facts.

Saanich bought an off-the-shelf solution as a quick fix—their stated motivation—an incoming tech-savvy Mayor. Senior staff wanted to move quickly to address some of the known IT vulnerabilities. So their stated goal was increased security. But they chose a program that is primarily an employee monitoring tool.

This was a solution that had a very limited effect on the district’s objective—improving IT security—yet had a very significant and detrimental effect on personal privacy.

This is because Saanich enabled invasive tools that captured an employee’s every keystroke and email, and pictures of screen activity every 30 seconds using a tool called Spector 360.

These tools vacuumed up not just work data, but also the private information of employees including, online banking transactions, confidential correspondence, and private passwords or images.

In addition, there was insufficient notification of employees that their computer activities were being monitored. The District’s standard terms of use policy failed to alert employees to the amount and type of personal information being collected.

There must be clear rules of engagement for collection and use of personal data. Notification is a legal requirement.

Ironically, Spector 360 created an additional security risk for the District, because it amassed a data haystack that would be of significant interest to parties with malicious intentions... and the District failed to implement any audit controls—no audit logs.

In short, the Mayor’s concerns about the use of the software were legitimate.

The software tools were privacy-intrusive and out of proportion to the threats Saanich had identified. It is the type of tool used in targeted workplace investigations when all other less intrusive measures have been exhausted. Installing keystroke logging, and screenshots every 30-seconds was an overreach with nominal effects on the security needs of the organization, but a significant privacy impact on employees.

Key Findings

My main recommendation in this report was that the District of Saanich DISABLE these key functions of their employee monitoring program and to delete all the data collected by the software.

I also recommended that Saanich appoint a chief privacy officer to lead the implementation of a comprehensive privacy management program for the District.

District and Council has agreed to implement all of my recommendations and agreed to delete all the data collected by the software.

The Saanich investigation made headlines – in BC and across Canada. But the best part... was that it clearly and unequivocally set the record straight. Employees do not check their privacy rights at the office door. Individuals have a reasonable expectation of privacy in the workplace, even when using a computer or mobile device supplied by an employer.

These rights were affirmed by the Supreme Court of Canada in *R v. Cole* and are enshrined in B.C.'s comprehensive privacy laws in the public AND private sector. Privacy law sets a very high threshold for the use of routine monitoring tools such as keyboard logging, workstation mirroring or tracking of personal messages.

Lessons from Saanich

So, what are the lessons for the CIOs in this room? How do you balance privacy and security?

First of all, I don't want you to think that you are OK because what Saanich did is something your company would never do.

"I wouldn't install Spector 360, so I don't have anything to worry about."

Wrong. This isn't a new problem – or a problem specific to Spector 360.

"Privacy. Oh yeah, we did that in 2005. We're good."

Wrong again.

Personal information protection has to be managed on an ONGOING basis. And it will never be as simple as picking a software tool off the shelf.

You have to get the BALANCE right between privacy and security.

What legitimate problem are you trying to solve? Is your chosen tool effective in addressing the problem? Are you transparent and open with your users?

The other thing Saanich got wrong that CIOs can learn from… was that the IT people did not talk to the privacy people.

The bottom line: privacy is a team sport – and everyone has a role to play in privacy compliance.

Rather than look at the Saanich report as an assessment of whether or not you have a problem… consider that this report creates an opportunity for you to lead.

You see, often times when I issue a detailed investigation report in a specific sector – – peer organizations in that sector take notice… it has a cascading effect… all of a sudden, the C-suite is paying a lot more attention to privacy and data security!

So I encourage you to take advantage of this opportunity to consider how well privacy and security play in your organization, and how it can be improved.

This is your opportunity to get proactive about privacy … before the regulators come calling!

Now is probably a good time to mention that my office has a new audit program.

Audit Program

It was a logical next step for us to add an audit function to our Office.

As a regulator, I am interested in taking an in-depth look at not only individual breaches and complaints, but also examining the CAPACITY of an organization to anticipate and respond to risks and threats. Do you have the policies, programs, systems and controls needed to manage privacy and information across an organization in a holistic way? Are your functions and teams working together?

We have published an audit charter that lays out a step-by-step process for how the Office will select audit targets, what information will be requested and the outcomes.

In January 2015 we released our first audit report, which was an assessment of core government's breach practices. The next phase is to examine privacy breach management and the privacy infrastructure of a health authority, a municipality and a university. We've begun in the health sector with a survey and interviews and have not yet selected which health authority to audit. Stay tuned for more from our audit program.

Accountability Guidance

You should also know that my office also has tools and guidance that can help all public bodies and private companies implement comprehensive privacy management programs...

Privacy management programs are PROACTIVE initiatives that will ensure you bake privacy in to your operations -- … creating a culture of privacy in your organization.

We've created guidance documents for both the public AND private sector that are essentially roadmaps to building privacy management.

These documents are scalable and practical. They work for SMEs and larger enterprises. They work for small public agencies and large government ministries.

They break privacy compliance down into simple steps.

If you follow them, you will have taken meaningful steps toward comprehensive privacy compliance, which is what Commissioners like me expect to see when assessing an organization's compliance with privacy law.

The guidance takes a "building block approach"—a maturity model to privacy management.

Beginning with a commitment to a culture of privacy. It has to start with tone from the 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. This is exactly where Saanich is starting now.

Once the foundation is laid, the next step is to develop and implement good privacy practices, procedures and systems. These are the building blocks of privacy management and include everything from privacy policies, to a privacy breach response plan, to training initiatives for your staff.

Once the building blocks are established, you need systems in place to monitor, assess and improve the program. You always need to be scanning your environment for changing threats and risk, but also gauging the effectiveness of your programs.

I'm not saying that if you implement a comprehensive privacy management program that you automatically receive a "get out of jail free" card. But, as a regulator in Canada where the accountability principle is emphasized in our law, the evidence of a privacy program will be a mitigating factor if you become subject to an investigation or a privacy breach.

This is where Saanich failed. I was deeply concerned to find no evidence of a privacy management program—no one in charge, no policy, no awareness of privacy obligations. In the wake of my report, they've committed to change that.

We are living in an information society. Until we have as much confidence in organizations' handling personal information as we do in banks safeguarding and using our money, I'll continue to promote and advocate for an accountability approach. And my office will continue to ask for evidence of privacy management programs in investigations of public bodies and private sector organizations.

A special note to those of you in the private sector: A special committee of the BC Legislature recently concluded a review of B.C.'s private sector privacy legislation, the *Personal Information Protection Act*. The committee recommended that B.C. add additional express legal requirements for privacy management programs prescribe in law. This will mean a mandatory requirement to publish privacy policies, train staff, and comprehensively plan for, and address, privacy across the organization.

The guidance documents I mentioned earlier are both available on our website. I encourage you all to take a look.

Having said all that... I would be interested in hearing from you about what steps your companies have taken to enact meaningful privacy controls... are CIOs being engaged in that process, are any of you taking the lead... are there any areas causing you concern, or where a regulator's gaze would be helpful? I look forward to our discussions over the course of the day.

I welcome your comments, or any questions that you have. Thank you for your attention this morning.