RICHARDS
BUELL
SUTTON LLP
Established in 1871

Posted on: May 21, 2020

AVOIDING AND MANAGING PRIVACY BREACHES IN REMOTE WORKING ENVIRONMENTS

By: RBS

COVID-19 has caused a fundamental shift in the way many of us work. Instead of being in an office, we are working from home. We no longer have our colleagues close by, we are working on our own computers and other devices, and we are trying to make do with less than ideal setups.

It also appears that remote work, at least part time, will be the new normal for the foreseeable future. Because of that, employers who did not have remote work policies in place should be thinking about how to create and implement them.

At the same time, every organization and public body will experience privacy breaches, and remote work has increased the risks. Knowing what a breach is, and being prepared for it, are key to both preventing breaches and limiting the damage when one happens.

Background: What is a Privacy Breach and Why Should I Care?

Under BC's privacy legislation (the *Personal Information Protection Act* for the private sector in BC, and the *Freedom of Information and Protection of Privacy Act* for the public sector in BC,) a privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of one or more person's information.

That person can be a client or an employee. The types of information can include:

- Names and contact information (emails, phone numbers, addresses);
- Financial information (SIN's, bank account information, payroll information); and
- Health information (clinical records, prescription information).

The information which falls within the legislation must be about a person. For example, a company's bank account information is not personal information. That kind of information is nonetheless sensitive. You may want to consider taking some of the steps for privacy breaches for this kind of information as well, as a matter of customer relations.

The most common types of privacy breaches are:

- Theft: through cyber attacks or theft of computers, hard drives, or memory sticks;
- Loss: an employee loses a computer, hard drive(s), or memory stick(s); and
- Accidental disclosure: an employee accidentally sends (e.g. by fax or email) personal information to the wrong person.

Employers should care about privacy breaches because they can impose substantial costs in dollars, time, and goodwill. Senior staff will have to devote time to investigating the breach and preparing new policies and procedures to prevent it from happening again. Hackers may demand a ransom to return information they have stolen. Investigation by the Office of the Information and Privacy Commissioner and lawsuits can result in additional legal costs and payouts to the individuals affected. Organizational reputations can be damaged, especially if the breach is not handled well.

What are the Risks with Remote Work?

The rapid move to remote work has highlighted the risks that already existed. These risks fall into four categories:

1. Failure to prepare remote work policies;
2. Employee training and error;
3. Improper use of technology; and
4. Compromised physical workspace.

Failure to Prepare Remote Work Policies

Remote work policies are important to prevent and manage privacy breaches because they force employers to think ahead and consider where the risks are, and how to manage them.

Many employers did not have remote work policies in place before COVID-19. These employers either moved to remote work without any policies, or set them up in very short order. Both of these situations lead to increased risk for breaches due to employee error, improper use of technology, or compromised physical workspace.

Employee Training and Error

Many breaches are, in part, due to failures in employee training and resulting employee errors. Someone clicks on the link in a fraudulent email, thinking it is in fact from their superior, and installs ransomware.

Someone else takes hard copy files home and then puts them in municipal recycling. Both of these situations can result in privacy breaches.

Employee training is vital to prevent and manage these breaches. Employees who have been trained on their organization’s remote work and privacy breach policies are less likely to make mistakes, and more likely to report a breach if it occurs.

Training is particularly important for remote workers, since there are more opportunities to make mistakes and fewer opportunities for supervision.

Improper Use of Technology

When most of us think of technology risks, we think of cyber attacks. Phishing and ransomware attacks in particular have been on the rise since the move to remote work. As noted above, employee training is key to preventing breaches as a result of cyber attack.

However, these are not the only technological risks. There are three, in particular, that arise from the rapid move to a remote work environment.

One risk is in relation to anti-virus and security software. When employees are working from an office, the employer is able to keep anti-virus and security software up to date on their work computers. If employees are now using home computers, they may need to update the software. Having out of date software increases the risk of cyber attack.

A second risk is in relation to unauthorized apps. We have all been looking for ways to work efficiently when our usual tools are not available. Some employees may choose to download and use apps – for example for smartphone scanning or videoconferencing – that have not been vetted by IT departments, resulting in security risks.

The third risk relates to use of free or inexpensive apps. Typically, when an app is free for the user, the developer earns income by gathering and selling information that is processed through the app. If the information includes personal information, this may be a privacy breach.

Compromised Physical Work Spaces

When employees are working from their employer’s office, the employer has control over their physical workspace. For instance, hard copy files with personal or sensitive information can be put away in locked cabinets or shredded when no longer needed. Calls or meetings with clients can take place in secure environments.

Employees working from home are in a much less secure environment. Many are working from kitchen tables, with other members of their household walking by and able to see their work or hear their calls. Sensitive papers may end up in municipal recycling. Either of these can result in a privacy breach.

What Can I Do To Avoid a Breach?

The two most important steps an organization or public body can take are to prepare thoughtful and thorough policies, and educate employees on them.

In particular, think about preventing cyber attacks, ensuring appropriate app use, and (to the extent possible) maintaining secure physical work spaces for employees. The details will depend on the nature of your work and the personal information you collect and use.

The Office of the Information and Privacy Commissioner for BC published a short and basic tips sheet to help employers set up remote working. It is available here.

How Can I Make Managing a Breach Easier?

Privacy breaches are inevitable. But you can take three steps to make them easier when they do happen.

1. Do the hard work now: prepare a breach protocol and train staff on it. For the breach protocol, think about:

- What kind of information is at risk and how sensitive it is;
- What kinds of breaches are likely to occur;
- How and to whom you want employees to report the breaches;
- Who will investigate and respond to the breach (in a large organization or public body, this may include the privacy officer, senior management, IT, security, and PR or communications) and how they will do so;
- What outside experts will be contacted and hired and when;
- How breaches will be contained;
- How and when individuals whose personal information was compromised will be notified; and
- Whether you have any obligations to notify anyone else (insurers, privacy commissioners, regulatory bodies, or commercial partners).

2. Contain the breach: do what you can, as quickly as you can, to limit the damage. For example,

unplug the computer that is transmitting data, or call the person who accidentally received the fax to ask them to shred it.

3. Contact counsel and your insurance broker early. Some organizations and public bodies have insurance coverage for cyber attacks and other privacy breaches. If you do, your insurer will appoint a breach coach to help you through the rest of the steps.