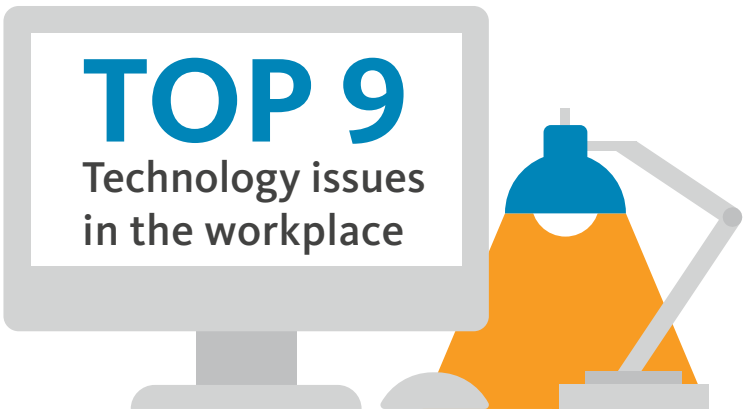
TOP 9
Technology issues in the workplace

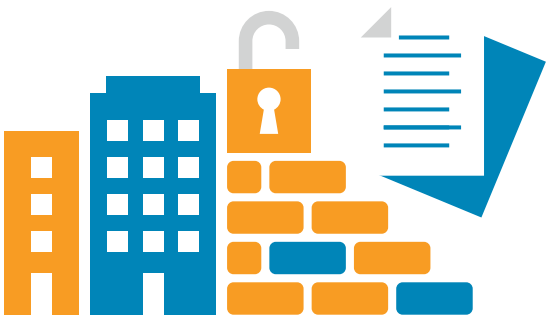


OSLER

Recent major data breaches from WikiLeaks to the Panama Papers have shed light on the potential risks regarding the ability of companies to protect electronic information and communications in the workplace. That's why employers need to be cognizant of the following nine possible issues so they can put in place the best preventative measures to avoid future problems.

1 Cybersecurity and data protection

Think the threats of a data breach only come from external sources or criminal hackers? Think again. The majority of cybersecurity breaches occur from mistakes by those who have access to a company's systems and breaches of data security come from the internal handling of company data.



Implementing sound policies and practices on data management in the workplace is crucial. Training employees around acceptable use, storage and retention of employer data, systems and property is of the utmost importance.

2 Employee misuse of social media

The scenario: An employee makes an inappropriate social media post that could reflect poorly on the employer. What can that employer do?

This could provide basis for the employer to discipline the employee, up to and including termination of employment. Several recent cases suggest termination with just cause is possible in these instances, especially when the post is potentially harmful to the employer.

3 When not to discipline for misuse of social media

But a word of caution: while it may be appropriate to discipline employees for the misuse of social media in some instances, in other cases it may not be.

Be prepared for different scenarios. Employees in Canada or the U.S. may argue that social media posts are protected, or that discipline is an unlawful reprisal under employment standards and other legislation.

4 Privacy on workplace computers

Most employees may think their personal workplace computers are their business only, but guess what? Employers may have the right to monitor their use.

Be clear about communicating and instituting workplace computer privacy policies that provide for employer monitoring, where the employer has a legitimate need to conduct monitoring and where such monitoring is reasonable in scope.

5 Bring your own device programs (BYOD)

The Canadian Privacy Commissioners have provided guidelines for organizations considering allowing employees to use their cell phones for both business and personal use. But instituting these BYOD programs also gives rise to certain associated risks.

When rolling out BYOD programs, employers must carefully consider the accompanying risks to privacy and security and be cognizant of the appropriate privacy guidelines, as well as best practices for protecting knowledge assets of an organization not protected by privacy legislation.

6 Social media background checks

Are there boundaries to conducting pre-hire social media background checks? Yes. These searches could give rise to privacy concerns including issues of consent and collection of irrelevant information.

Be mindful of the circumstances surrounding such background checks and the associated guidelines. The checks must be conducted in accordance with guidance from Canadian privacy commissioners, and must be reasonable in the circumstances of the employer's operations.

7 Educating employees on e-discovery

The scenario: an employee texts or e-mails a co-worker some confidential information instead of using the phone. While this may be seemingly harmless, they need to know the risks of such communication.

Be mindful of the paper trail. It's important to educate employees about the potential hazards surrounding electronically stored information. The employee needs to be aware that what they write could be produced in subsequent litigation.

8 Protecting your client list from employees' online presence

If an employee with a social media account that functions as a client list or company contact point leaves their job, who owns the account? It's a bit of a grey area.

Institute a concrete social media policy that covers this. To avoid the possibility of undermining contractual non-competition, employers should take concrete steps to establish corporate ownership of social media accounts that are used for business purposes.

9 Updating policies

The changing digital landscape means it's crucial for businesses to be cognizant of ongoing technological developments to ensure their security policies are up-to-date.

Regular revision and education of privacy policies is key. Updating any policies relating to email, Internet, social media, travel and passwords, electronic devices or BYOD, and acceptable use is critical, while educating employees on phishing emails and other nefarious communications is equally important. Industry Groups should share key security threats and responses.

FOR MORE INFORMATION, CONTACT:

Brian Thiessen | Employment & Labour and Privacy & Data Management
bthiessen@osler.com

Rachel St. John | Associate, Privacy & Data Management
rstjohn@osler.com

Osler, Hoskin & Harcourt LLP
Toronto Montréal Calgary Ottawa Vancouver New York | **osler.com**