

Overview

- Cyber Challenges for Employers
- Activities by employees – cause for concern
- Workplace Policies: Establishing and Enforcing Ethical Standards
- Case law developments

Social Media

- Addressing the impact of social media is but one of many cyber challenges facing employers today
- Social media - on-line communications in which individuals are author and/or audience
- Utilize software that enables anyone to post, comment, share and form communities
- Uninterrupted connectivity 24/7
- No boundaries

Why Should We Be Concerned About It?

- Lost productivity
- Inability to Manage
- Corporate liability
 - Harassment
 - Copyright
- Damaged reputation
- Lost customers
- Lost shareholders
- Share devaluation



Do we need some new laws?

- No!
- Medium is new, but
- Issues and law remain the same

The Law

- No need for new law – legal principles exist to deal with these scenarios
- New application of existing legal principles
 - Personal use is no different than previous example of “slacking”
 - Email/FaceBook harassment is same as earlier forms of harassment
- No expectation of privacy

The Concerns

Cyberslacking

- Staff with FaceBook open all day
- Hours & hours online



The Concerns

- Liberal party staff being “friend” of Stephen Harper
- Microsoft employee posting pic of Macs delivered to Microsoft offices
- Blog posts revealing confidential info of company, colleagues & clients



The Concerns

- Others can “share” info about you
 - “I partied hard with Jimmy last night and there’s no way he’s making it to work today”
 - pictures
- Joining groups
 - “I Support Hudak”
 - “I love Tim Hortons”
- Creating/joining events
 - “Sam’s 50th Birthday Blowout”
 - “Rally Against The War in Afghanistan”



The Concerns

FaceBook post:



The Concerns

- Employee dismissed for cause based on poor performance
- Manager gave him recommendation on LinkedIn the week before dismissal



- Now suing for wrongful dismissal



Using Social Networking For Good

- Monitor employee behaviour
 - Abuse of sick leave/disability
 - Competing with employer
- Mitigation issues
 - Available jobs
 - Proof of mitigation



“Let’s Ban Facebook”

- 2009 University of Melbourne study found surfing the net at work for pleasure increases concentration levels and makes workers more productive
(Media Release April 2, 2009 www.unimelb.edu.au/news/5750)
- Can be used for valid business reasons: blanket policy not always advisable



Using Social Networking For Good

- Screening Applicants
 - Google
 - Social networking sites
 - Be realistic (we all have those bad photos out there somewhere!)



But Be Careful

- Online research can reveal protected grounds
 - Race
 - Age
 - Disability
- Screen candidates in consistent manner
- Have non-decision maker filter out inappropriate info
- Do not “friend” candidates or demand access
- Log reasons for not hiring



Post-Dismissal

- Use social media to monitor mitigation
- Log and share job opportunities
- Learn when individual has mitigated



Workplace Policies:

Establishing and Enforcing Ethical Standards



Workplace Policies (cont'd)

May:

- Protect the organization and its human resources
- Define appropriate conduct and express organizational values
- Establish/maintain the organization’s status as an employer of choice
- Be enforceable



Workplace Policies (cont'd)

Background:

- Workplace policies governing conduct not “new” in Canadian workplace context (eg. No fighting rules)
- Labour and employment legislation may either necessitate the development and posting of a policy, or render it unnecessary
eg. Bill 168 amended OHS and requires employers to develop and implement Workplace Violence and Workplace Harassment policies



Workplace Policies (cont'd)

Background (cont'd)

- Historically, impetus for development of workplace policies was promotion of safety and efficiency
- Recent impetus fueled by corporate scandal/dishonesty and the regulatory response
eg. “Sarbanes-Oxley” (2002): U.S. legislation tightened federal controls over accounting industry and dictated improved corporation governance, including codes of conduct and whistle-blower protection



Workplace Policies (cont'd)

Background (cont'd)

- In 2005 Canadian Securities Administrators (CSA) released National Instrument 58-101, requiring reporting issues to disclose whether board of directors has adopted a written code of business conduct and ethics for the organization’s directors, officers and employees
- Board of directors must “encourage and promote a culture of ethical conduct”



Workplace Policies (cont'd)

Protecting the Organization

- Policy governing appropriate use of technology may assist an organization to minimize: leakage of confidential information; theft of time; viewing, downloading and distribution of pornography and sexually-explicit content; workplace violence and harassment
- Appropriate Use of Technology Policy may be a stand alone policy or part of a “code of conduct”



Workplace Policies (cont'd)

Protecting the Organization (cont'd)

- **Problem:** in a world of 24/7 connectivity, separation of work and play is not a bright line
- Does employer have a right to govern employees’ conduct at work, and off-duty?
- Workplace is a microcosm of the bigger world: why should employees be less ethically lax than the public at large?



Workplace Cyber Misconduct: Written Policies

1. Produce a *written policy and seek to include it as part of the employment contract
 2. Communicate / publicize the policy
 3. Monitor use of technology and workplace behaviour
 4. Discipline violators
 5. Continuously update policy as technology evolves
- (* or policies)



Workplace Cyber Misconduct (cont'd)

- Putting aside the issue of enforceability, it's better to have an Appropriate Use of Technology Policy than to not have one
- Elements of an Appropriate Use of Technology Policy:
 - Define the equipment/hardware and networks covered by policy
 - Employer asserts ownership over equipment / networks that it owns/leases, and that are used/accessed by employees



Workplace Cyber Misconduct (cont'd)

- Elements of an Appropriate Use of Technology Policy (cont'd)
 - Employee has no reasonable expectation of privacy
 - Identify limits of non-business related use of equipments and networks
 - Enforcement mechanisms



Workplace Cyber Misconduct (cont'd)

Poliquin v. Devon Canada Corporation
2009 ABCA 216 (“Poliquin”)

- Devon Canada terminated Mr. Poliquin's employment following an investigation that revealed he had accepted services from a company supplier, and had used employer's computer equipment and Internet access to view and transmit racist and pornographic material



Workplace Cyber Misconduct (cont'd)

Poliquin (cont'd)

- Violated corporate policies, including the code of conduct
- Non-union employee
- Devon Canada terminated his employment for cause



Workplace Cyber Misconduct (cont'd)

Poliquin (cont'd)

- Alberta Court of Appeal:
 - Code of Conduct was an essential part of employment contract
 - Code of Conduct comprised of several corporate policies that Mr. Poliquin breached, including Information Systems Usage Policy and Harassment and Violence Prevention Policy
 - Breach of trust inherent in employment relationship
 - Employer policies are relevant, as part of circumstances surrounding dismissal, but are not determinative of answer to “just cause” question



Workplace Cyber Misconduct (cont'd)

Poliquin (cont'd)

- “It is important to situate a document like the Code of Conduct in the larger workplace context. Employers have the right to set the ethical, professional and operational standards for their workplaces. Doing so not only falls within an employer's management rights, it also constitutes an integral component of good corporate governance.”



Workplace Cyber Misconduct (cont'd)

Poliquin (cont'd)

- “The workplace is not an employee’s home; and employees have no reasonable expectation of privacy in their workplace computers. It therefore follows that while employers may permit employees limited personal use of workplace computers, the employer is entitled to restrict the terms and conditions on which that use is permitted.”



Workplace Cyber Misconduct (cont'd)

Employer Policies and Practices

Enforcement considerations:

- √ policies are part of employees’ terms and conditions of employment (pros and cons for employer)
- √ policies communicated clearly and unambiguously



Workplace Cyber Misconduct (cont'd)

Employer Policies and Practices

Enforcement considerations (cont'd):

- √ full and fair investigation of alleged wrongdoing
- √ prompt, consistent and equitable enforcement of policies



Cyber Challenges II