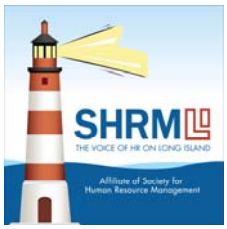
jackson lewis
Preventive Strategies and Positive Solutions for the Workplace®



'Tis The Season – Lost Productivity & Cyber-Threats

On Cyber Monday (the Monday after Thanksgiving), online shoppers can snag their desired holiday gifts from behind a computer screen without having to brave the crowds of Black Friday. Unfortunately, many of these shoppers will be at work while they shop. This online activity results in a significant loss in productivity for employers throughout the country. For example, it is estimated that Cyber Monday 2010 cost employers an estimated $580 million in lost productivity.[1] That's one day!

To make matters worse for employers, the online purchasing-frenzy does not end when the clock strikes midnight. Rather, it lasts the duration of the holiday season … and issues associated with the holiday Cyber-shopping phenomenon are growing. Prior to the 2011 holiday season, half of all American workers admitted they planned to shop online during work hours.[2] Of those, 34% said they would spend 1 hour or more shopping (up from 27% in 2010) and 16% said they would spend 2 or more hours shopping (up from 13% in 2010).[3] Plus, many Cyber Monday retailers offer a "deal of the hour" available only for 60 minutes during the day – practically forcing deal-seeking employees to put work tasks aside to shop from work.[4]

The above realities pose many risks to employers, but none greater than significant loss of employee productivity and the increased risk of Cyber-threats, such as computer viruses, that can compromise an employer's electronic communications systems.

---

[1] Benefit Focus, *Cyber Monday Is Here! Is Your Workplace Prepared?* (Nov. 29, 2010), *available at* http://www.benefitfocus.com/blogs/your-hr-blend/2010/11/29/cyber-monday-is-here/.

[2] Tom Starner, *Accommodating Cyber Shopping*, HUMAN RESOURCE EXECUTIVE ONLINE (Dec. 2, 2011), *available at* http://www.hreonline.com/HRE/view/story.jhtml?id=533343780 [hereinafter HRE ONLINE Article].

[3] *Id.*

[4] National Retail Federation, *Cyber Monday Significance Rises as Nine in Ten Retailers Plan Special Promotions* (Nov. 22, 2010), *available at* http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=1040.

Preparing for these risks does not make an employer Ebenezer Scrooge. Rather, such risk management reinforces an employer's commitment to the goals of the business while at the same time protects critical electronic communication systems from external threats.

I. Best Practices For Addressing Decreased Productivity

Employers looking to curtail lost productivity resulting from on-line shopping during the holiday season must give serious thought to adopting an electronic communications policy that provides necessary protections to stymie online shopping in the workplace or reviewing and refining current policy. While an electronic communications policy may not eliminate the risks and challenges posed by employees' unauthorized communications, a policy that is well-drafted and reviewed for legal compliance provides employers with safeguards. In drafting/auditing such a policy, employers should consider the following:

- Ensuring that the electronic communications policy encompasses all of the employer's communication systems including voice, internet, and e-mail;
- Ensuring that the policy's restrictions on usage are reasonable, enforceable and unambiguous. For example, an absolute prohibition on using the Internet during work hours is the wrong approach if the employer routinely permits employees to use the Internet for personal reasons provided such usage does not interfere with productivity;
- Ensuring that the policy provides the employer with the right to monitor, record or access electronic communications on its systems, specifically employee internet usage;

- Ensuring that the policy advises employees that they have no expectation of privacy in communications on the systems (except as otherwise provided under applicable law); and
- Specify restrictions on downloading content from the Internet.

Employers must remember that policies that restrict employee use of the Internet and email to business use only may run afoul of the National Labor Relations Act. The National Labor Relations Board takes the position that general blanket prohibitions on the use of such electronic communication systems which extend into non-work hours may violate no-solicitation and no-distribution rules, if discriminatorily applied. That is, if an employer generally allows personal use of internet usage but then denies access or disciplines an employee when an employee is accessing union-related websites, the Board may find the policy is being discriminatorily enforced.

There is no better time than the present to refine, re-circulate (or issue) an electronic communication policy and remind employees of their obligations.

As an alternative to a comprehensive electronic communications policy, more and more employers also are choosing to block Internet access in its entirety at employee workstations, or permit only websites that are business-related. As of 2011, 60% of all U.S. employers blocked employees' access to online shopping sites in the workplace (up from 48% in 2010). Similarly, more and more employers are proactively monitoring employee Internet usage during the work day in an effort to identify abuse and curb usage. As of 2011, an estimated 50%

of all American employers monitor employee internet (up from 47% in 2010).[5] A more rigorous blocking or monitoring procedure may be the appropriate approach for your workplace.

II. Protecting Your Electronic Systems From Harm

In addition to the productivity concern, online shopping exposes employers to outside threats as employee consumers using the employer's system to shop are ideal prey for computer viruses. During the holiday season, the allure of finding the perfect deal or "flash sale" may cause typically-vigilant employees to let their guard down. As such, employers should plan ahead by taking the following precautions:

- Ask your IT department to notify employees of specific security threats such as fake e-cards and scams like ads promising free gifts with purchase;
- Ensure anti-virus software is up-to-date;
- Caution employees to avoid providing a work email address as contact information; and
- Advise employees to notify IT or HR immediately if they receive an unsolicited offer in their email; instruct them not to open or even click on the message.

* * *

As always, feel free to contact Chris Valentino (631-247-4653), Ana Shields (631-247-4657) or John Porta (631-247-4650) of Jackson Lewis LLP with questions.

[5] National Retail Federation, *Cyber Monday Significance Rises as Nine in Ten Retailers Plan Special Promotions* (Nov. 22, 2010), *available at* http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=1040.