

**CYBERCRIME** means an incursion, intrusion, penetration, impairment, use or attack of a COMPUTER SYSTEM(S) by electronic means by a third party, other than the INSURED or the INSURED'S LAW FIRM.

**COMPUTER SYSTEM** means any electronic device, component, network or system, or any protocol, portal, storage device, media, or electronic document, or any computer software, firmware or microcode, or any associated technology which receives, processes, stores, transmits or retrieves data either locally or remotely, or any part thereof, whether stand-alone, interconnected or operating as part of an integrated system or process, for use by or on behalf of the INSURED and/or the INSURED'S LAW FIRM.

## The LAWPRO

# \$250,000 cybercrime coverage:

## What it covers and why

As of the 2014 policy year, the LAWPRO mandatory insurance program will include express coverage in the amount of \$250,000 for losses related to cybercrime, as defined in the policy. This sublimit (or cap) of coverage provides a modest "safety net" for lawyers in the area of cybercrime exposure. We say modest because like the fraud risks the profession has faced over the years, there is no way to predict the total possible exposure, and prevention is a far better tool to deal with this societal risk than insurance.

In the specialized world of Canadian lawyers' professional indemnity insurance, the most common approach so far has been to expressly exclude coverage for cybercrime losses. In considering what LAWPRO program protection should be made available to Ontario lawyers in 2014 regarding claims involving cybercrime, and what steps should be taken to better ensure that lawyers and law firms are aware of this growing exposure and what they might do to better protect their clients and themselves, consideration has been given to:

- The threat that cybercrime represents to clients and the viability of law practices in Ontario;
- The limited technology resources adopted to date by many members of the bar to comprehensively address cybercrime risks;
- The increasing availability of commercial business insurance to address the broader aspects of cyber risks;
- The growing and evolving nature of cyber risks and related need for increased awareness and active risk management by lawyers and law firms;
- The choices and options available to lawyers and law firms to reduce their vulnerability to cybercrime through adopting technology and security best practices;
- The potential impact of a systemic or catastrophic loss on the LAWPRO program and premiums charged to lawyers, especially if a group of law firms experiences a loss; and
- The need for LAWPRO to continue operating in a commercially reasonable manner and ensuring that risk-rating is maintained.

In late 2012, LAWPRO learned of a high-value cyber attack on an Ontario firm. The attack was highly sophisticated and complex, and was designed to permit the fraudster to gain direct access to a firm's trust account using online banking privileges. This attack, and media reports of many others, have served to demonstrate the potential exposure of the insurance program to losses arising out of cybercrime.

After careful consideration of the potential risk, including the potential for clusters of such claims across law firms, it became clear to us that a two-pronged response was warranted. For the 2014 policy year, we have opted to 1) explicitly address cybercrime risk in the mandatory insurance program policy, and 2) take steps to educate the bar about cyber risks and to recommend that all lawyers take active steps to prevent cybercrime before it happens.

Thus, as of the 2014 policy year, the LAWPRO mandatory insurance program will include a sublimit of coverage in the amount of \$250,000 for losses related to cybercrime as defined in the policy. See the sidebar for the definition of cybercrime, and the related definition of a computer system.

The LAWPRO insurance coverage for cybercrime claims is only one of several aspects of a fulsome and responsible response to a complex problem. We urge you to carefully reflect on the extent to which, despite the coverage available under our policy, you remain vulnerable to the potentially serious consequences of a cyber attack.

Remember that any losses from cybercrime that are not connected with the provision of professional legal services will not be covered under the LAWPRO policy. These losses could include damage to equipment or software, business interruption, and reputational harm. See "Other cyber risk insurance options: Do you have the coverage you need?" on page 26 for a basic overview of other types of insurance that firms may wish to consider to cover those risks or loss amounts that fall outside the LAWPRO policy.

However, even where a firm chooses to obtain other coverage, insurance against cyber losses should be viewed as a worst-case remedy, and not a regime of prevention. If businesses insure themselves without taking active steps to secure their computers and networks, cyber criminals will continue their efforts undeterred.

Law firms and individual staff members and lawyers who work in them must educate themselves about cyber risks and take all reasonable steps to ensure that data and funds are securely protected. We hope that the content in this issue will serve as a useful resource in that regard. ■

© 2013 Lawyers' Professional Indemnity Company. This article originally appeared in LAWPRO Magazine

"Cybercrime and Law Firms (Vol. 12 no. 4). It is available at [www.lawpro.ca/magazinearchives](http://www.lawpro.ca/magazinearchives)

The practicePRO and TitlePLUS programs are provided by LAWPRO