IADC COMMITTEE NEWSLETTER

PROFESSIONAL LIABILITY

NOVEMBER 2018

IN THIS ISSUE

This paper briefly reviews expanding cyber liability around the world which arises in part from recent legislation such as the GDPR in the EU, PIPEA in Canada, and the Digital Privacy Act that came into force in Canada on November 1, 2018. It examines the gaps in coverage that may exists for business and professionals and particularly real estate brokers in British Columbia under their E&O and CGL policies. It is a cautionary tale for all professionals, including law firms.

Cyber Insurance Coverage in Canada

ABOUT THE AUTHOR

Harmon C. Hayden is internationally recognized as one of the world's leading lawyers in insurance, reinsurance, and product liability. He has served as a nominee of the Attorney General of Canada on the Minister's Judicial Advisory Committee and has appeared in the Supreme Court of Canada in *EDG v. Hammer* [2003] S.C.R. 459 (one of a trilogy of cases heard at the same time regarding institutional liability for sexual abuse). He has published and lectured extensively, and has served as an Adjunct Professor of Insurance Law, Faculty of Law, at Thompson Rivers University. He can be reached at harmon.hayden@haydenlaw.ca.

ABOUT THE COMMITTEE

The Professional Liability Committee consists of lawyers who represent professionals in matters arising from their provision of professional services to their clients. Such professionals include, but are not limited to, lawyers, accountants, corporate directors and officers, insurance brokers and agents, real estate brokers and agents and appraisers. The Committee serves to: (1) update its members on the latest developments in the law and in the insurance industry; (2) publish newsletters and Journal articles regarding professional liability matters; and (3) present educational seminars to the IADC membership at large, the Committee membership, and the insurance industry. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Matthew S. Marrone
Vice Chair of Publications
Goldberg Segalla LLP
mmarrone@goldbergsegalla.com

Businesses and professionals are facing unprecedented cyber risks and increasing exposure. Data breaches are becoming more widespread and the legal and financial risks are increasing. Many large corporations such as Sony and Yahoo have been subject to extensive hacking. Countless small businesses and professionals have been attacked as well. There are Advanced Persistent Threats carried out by hacking groups for business and political reasons. Organized crime groups and industrial spies use social engineering, spam, phishing, spyware, malware for identity theft or fraud to gain unauthorised access to the data systems of organizations and businesses. Then there are simply the unorganized criminals and hackers intent on money or mayhem. Data has a black-market value.

All of these threats have given rise to a plethora of litigation, including class actions. The legal costs alone can be ruinous. Such data breach cases can arise simply because of administrative error by organizations disclosing personal or confidential information by accident.

In addition to these risks, there has been a host of legislative changes that have produced previously unknown exposures on businesses and professionals. In Canada, this has included the federal Personal Information Protection and Electronic Documents Act, SC 2000, c.5, and provincial laws deemed to be substantially similar. There are provincial Privacy Acts providing for statutory rights of action for breach of privacy. As of July 1, 2017, the federal Canadian Anti-Spam Legislation, SC 2010, c. 23 (CASL), has provided for personal rights to sue for damages where the legislation has been breached. Under the CASL, fines for non-compliance can range up to $10 million. Private rights of action are limited to $200 per contravention.

Internationally, Europe's General Data Protection Regulation has come into force. It casts a very wide net, applying to any company that offers goods or services to EU residents, even if they are based in Canada. Data protection authorities can fine violators four per cent of their global revenue or 20 million Euros. One would hope that such penalties are reserved for the most egregious of offenders.

Most recently, the Digital Privacy Act, SC 2015, c. 32, came into force November 1, 2018 in Canada. A useful summary of this legislation as follows:

WHAT IT IS

Simply put, the amendments coming into force on the 1st November now make it mandatory for applicable organizations in Canada to notify in cases where a privacy breach creates "a real risk of significant harm to the individual," and to maintain a record of every privacy breach that the organization suffers.

WHO IT WILL APPLY TO

The changes will apply to all those organizations with pre-existing obligations under PIPEDA. This means that any commercial (for profit) organization that uses, collects or discloses personal information in the course of their business activities will have to comply. PIPEDA does not generally apply to not-for-profit organizations or those commercial organizations operating in regions (Alberta, British Columbia & Quebec) where provincial laws have been deemed substantially similar to PIPEDA, unless the personal information that they hold crosses provincial or national borders.

WHAT IT WILL REQUIRE ORGANISATIONS TO DO

The Digital Privacy Act will require applicable organizations to notify affected individuals and the Commissioner of privacy breaches that are likely to cause a "real risk of significant harm to the individual." "Significant harm" is deemed to include, amongst other things, humiliation, damage to reputation or relationships and identity theft. Deciding on what constitutes "a real risk" requires reflection on the sensitivity of the information in question, the likelihood of misuse and any other prescribed factor.

In those cases where a privacy breach creates a real risk of significant harm, organizations must give notice "as soon as feasible" after the breach has been discovered. Notification can be given "in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances." The information a notification needs to contain differs between those that are sent to the Commissioner and those that are sent to affected individuals, but the content requirements common to both include:

- *A description around the circumstances of the breach, including the day on which, or the period during which, the breach occurred;*
- *A description of the personal information affected by the breach;*
- *A description of the steps the organization has taken to reduce the risk of harm that could arise from the breach;*
- *Contact information to allow either the Commissioner or an affected individual to find out more about the breach.*

CONCLUSION

The introduction of these notification and record-keeping requirements marks a significant change to the legislative environment in Canada, and those organizations affected will have to make sure that they are aware of their obligations under act, because failure to comply can result in fines of up to $100,000 per offence.

That said, although this is an important change, it is important to note that dealing with a data breach isn't the only cyber risk that businesses face. Canadian organizations have had to deal with cyber risks for some

time now, and there has already been a large number of cyber insurance claims in Canada for issues like cybercrime and system business interruption. The Digital Privacy Act adds to these exposures, but it certainly doesn't replace them. It also doesn't mean that those entities that are not subject to PIPEDA are free from cyber risk.

And while these changes will increase the privacy risk for organizations in Canada, it is unlikely that this will result in a US-style privacy landscape anytime soon. US legislation, regulatory appetite and litigation culture are still very different when compared to Canada.

In view of this increasing risk, The Insurance Bureau of Canada advises as follows:

Speciality insurance coverage for cyber liability risks is relatively new to the marketplace. The possibility of cyber liability lawsuits is a reality that every business owner should consider. There have been several very high-profile personal information breaches that affected tens of millions of records and will cost the companies involved millions of dollars.

If you rely on an online presence and use e-commerce as a method of distribution or have employees who carry electronics that hold customers' personal/commercial information, your insurance representative can help you find coverage that will protect your organization.

If you are a small business, a professional, or a real estate broker, you may think that you have adequate insurance coverage for the expanding risks of cyber liability. In most cases, it is probably fair to say that you would be wrong. Coverage under existing non-cyber liability policies contain either huge gaps in coverage or no coverage at all for expanding cyber risks.

In some professional E&O policies, such as the BC Lawyers Compulsory Professional Liability Policy, some of the exclusions may be more specific such as this:

This policy does not apply to:

. . .

13. a claim arising out of or in way connected to the collection, use and/or disclosure of any information to a third party, or the receipt by or transmission to a third party of malware or malicious code.

As most readers will know, the duty to defend under a liability policy is separate and distinct from the duty to indemnify. The pleadings govern the duty to defend. If the claim alleges a state of facts which, if proven, would fall within coverage, the insurer will have a duty to defend. There are many cases in which some claims may be within coverage and some outside of coverage. In most such cases, the insurer will be required to defend the claim in its entirety, notwithstanding that some claims are outside of coverage. It is entirely possible to envision a set of facts in which a real estate broker is faced with claims "arising from their errors in performing or failing to

perform real estate services for others" which also include claims for cyber liability, such as administrative errors in disclosing personal or confidential information which results in damage to a client.

Some may take solace in the fact that they may have a commercial policy that provides for both first party and third-party exposures, those that do not fall under the professional E&O policy. The standard property coverage of a commercial policy, however, will exclude "data problems". Such is frequently defined as the "erasure, destruction, corruption, misappropriation, or misinterpretation of data", or errors relating to "creating, amending, entering, deleting or using data".

However analysed, the vast majority of professional E&O policies and commercial policies, for both first party and third-party losses will be very limited or provide no coverage for cyber risks. In view of this limited coverage, the markets have responded with creating various policies to respond to cyber risks.

I would recommend that any insured should consult with their broker to review their personal risks, exposure and their existing insurance coverage. All of my research leads me to believe that a reasonable business owner or professional should consider cyber liability insurance.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

MAY 2018
When Eating Crow is the Best Item on the Menu: Stipulating to Liability in Professional Liability Actions
Luke Sbarra and Tom Buckley

A Lawyer's Duty to Inform a Client of Errors Made in Representation
Josh Neighbors and Tom Buckley

MARCH 2018
Quandaries and Quagmires: Legal Ethics and Risk Issues as of January 2018
Chuck Lundberg

SEPTEMBER 2017
Clients Barred from Blaming Lawyer for Consequences of Clients' Illegal, Immoral or Wrongful Conduct: North Carolina Court of Appeals Reaffirms In Pari Delicto Defense in Legal Malpractice Actions
William Graebe and Dan Zureich

JANUARY 2016
No 'Good Reason' for a Second Bite at the Apple: Recent Nevada Supreme Court Decision on Nonmutual Claim Preclusion May Prove Useful for Legal Malpractice Defense Counsel
Erin K. Higgins, Andrew R. Dennington and Kathleen R. O'Toole

MARCH 2015
The Year of the Cyber Breach
Elizabeth S. Fitch and Theodore M. Schaer

FEBRUARY 2015
The Tide Has Turned: An Update Regarding the Evolution of the Intra-Firm Attorney-Client Privilege
Charles Lundberg and Aram Desteian

JANUARY 2015
Cybersecurity: The Continuing Evolution of Insurance and Ethics
Dan Zureich and William Graebe

OCTOBER 2014
An Attorneys Duty to Disclose Evidence to Opposing Counsel
Michael E. Brown