LA TURQUOISE

intact ASSURANCE

Mortgage brokers

Cybersecurity coverage included*

MORTGAGE PROFESSIONALS CANADA

In addition to the professional liability coverage offered as part of our program for mortgage firms and brokers, these additional coverages are offered by Intact Insurance.

GUARANTEES AND LIMITS

Information security and privacy liability coverage (3rd party)	**$ 500 000**
Professional Liability cyber expense coverage (1st party)	**$ 250 000**
Extortion**	**Basic : $ 10 000** **Option : $ 25 000**
Social engineering**	**$ 10 000**

PREMIUM

Members	**$ 110**
Non-members	**$ 150**
$ 25 000 extortion payments	**$ 15**

* Coverages are subject to the exclusions, definitions and conditions of the endorsements and the policy.
** These coverages are available only if the policyholder qualifies for them.

EXTORTION AND SOCIAL ENGINEERING QUALIFICATION

SOCIAL ENGINEERING

- In compliance with your security protocol, is an authorization requiring the approval of at least two people required to make a transfer?
- If the answer to the previous question is no, can more than one person make a transfer and/or sign a cheque?
- Does the policyholder confirm each request to change supplier or customer account information by a call using only the contact number previously provided by the customer prior to receipt of the request, and is this confirmation completed before the change is made?

EXTORTION

- Does your organization back up its systems on a regular basis?
- Does your organization protect its systems with anti-virus software?
- Does your organization encrypt its system data and digital content?
- Has your organization implemented multi-factor authentication?
- Does your organization have a program for updating software and applying fixes on a regular basis?
- Does your organization provide its employees with training on cybersecurity risks and social engineering scams at least once a year?

INFORMATION SECURITY AND PRIVACY LIABILITY COVERAGE
(3rd party)

Coverage for defence costs and losses caused by a breach of confidentiality. The insurer agrees to pay, on behalf of the policyholder, all amounts which the policyholder is legally obligated to pay as a result of a first claim made against it during the policy period for losses arising from:

INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS

Unauthorized use or infringement of intellectual property contained in electronic or digital form.

NETWORK-RELATED PERSONAL INJURY

The electronic or digital publication or dissemination of libellous, slanderous or defamatory content.

* Coverages are subject to the exclusions, definitions and conditions of the endorsements and the policy.

BREACH OF SECURITY AND CONFIDENTIALITY

Failure to warn of:

- unauthorized access to or disclosure of confidential or personal information owned, managed or held by a policyholder or entrusted to them;
- unauthorized installation or dissemination of a computer virus or similar program;

or

- unauthorized access to or use of any computer hardware or network, software or electronic information system.

PROFESSIONAL LIABILITY CYBER EXPENSE COVERAGE
(1st party)

Coverage for direct damages (costs of notification and management of confidentiality breaches) for three key categories: **remediation costs, legal advice costs, data recovery and restoration costs.**

Costs for notification and management of breaches of confidentiality

REMEDIATION COSTS

Remediation costs covered under the notification and breach management expenses include necessary and reasonable costs incurred by the company for the purpose of notifying its customers of a breach of confidentiality of changes to account numbers and security codes, computer investigation services, public relations services retained by the company as a result of the breach, and credit and fraud monitoring services.

LEGAL ADVICE COSTS

Costs incurred by the policyholder for the purpose of retaining the services of a lawyer to respond to law enforcement authorities or investigators.

DATA RECOVERY AND RESTORATION COSTS

Costs include those associated with the recovery and restoration of data (belonging to a third party but entrusted to or held by the policyholder) and resulting directly from a breach of confidentiality.

* Coverages are subject to the exclusions, definitions and conditions of the endorsements and the policy.

SOCIAL ENGINEERING

COVERAGE FOR SOCIAL ENGINEERING FRAUD

The insurer will compensate the policyholder for losses arising directly from the transfer, payment or delivery by the policyholder of money, securities or other valuables as a direct result of social engineering fraud committed by a person claiming to be a supplier, a customer or an employee authorized by the policyholder to give instructions to other employees or to the policyholder (if the policyholder shown on the Declarations Page is a natural person who is the sole proprietor) in order to transfer money, securities or other valuables if such fraud occurs and is first discovered during the insurance period.

Example of a claim

THE FACTS

The policyholder receives an e-mail from a fraudster claiming to be their supplier, asking them to change their banking information. The policyholder makes the payment. A short time later, the real supplier writes to inform the policyholder that they have not received their payment of $18 522.

ACTION PLAN

The policyholder was contacted immediately after receiving notice of the incident from the broker. They provided concrete proof, such as payment statements, e-mail exchanges with the fraudster, specimen cheques and detailed invoices. The policyholder would be entitled to reimbursement in accordance with the policy limit.

RESPONSE SERVICE

24/7 response and support service by Cyberscout.

Details to come.

DIFFERENCES BETWEEN OUR PRODUCT AND SINGLE-LINE CYBERSECURITY INSURANCE

Variable premiums starting at around $600 and additional coverage:

- Higher limits available
- Business interruption
- Regulatory defence and penalties
- Replacement of IT equipment and bricking coverage
- Certain cybercrime coverage, including funds transfer fraud and invoice manipulation

* Coverages are subject to the exclusions, definitions and conditions of the endorsements and the policy.

EXTORTION PAYMENTS

COVERAGE FOR EXTORTION PAYMENTS

Upon receipt of satisfactory proof of payment by the policyholder, the insurer will reimburse extortion payments made by the policyholder or on its behalf through a supplier selected and approved in writing by the insurer to provide services to the policyholder as a result of extortion occurring and first discovered during the policy period.

Example of claim

THE FACTS

The policyholder has discovered that a number of its employees were unable to connect to their computers. In addition, several of their files had been altered. Later that day, hackers left a voicemail stating that they had encrypted their files and would unlock them only if the policyholder paid their ransom demand, and they threatened to publish the data on the dark web. The hacker encrypted the policyholder's main server as well as some backups.

ACTION PLAN

The policyholder was contacted immediately by the broker after it received notice of the incident. An outside firm was retained to provide legal advice and determine whether there had been exfiltration of confidential data. The forensic firm's report showed that there had been a breach of confidentiality. In addition, the hacker made a demand for ransom to recover the files. This is clearly a case of extortion. After obtaining the insurer's approval, the policyholder would be entitled to reimbursement within the limits of the policy.