RIBO

REGISTERED INSURANCE BROKERS OF ONTARIO

PRINCIPAL BROKER HANDBOOK SUPPLEMENTARY RESOURCES: **CYBER SECURITY**

RIBO recommends that firms adopt a cyber security program that outlines cyber security policies and procedures to protect against cyber-attacks. Reports have noted massive increases in the number and severity of cyber-attacks experienced by businesses of all sizes. These attacks are expected to continue increasing as businesses rely on digital platforms and as more employees work from home on a regular basis. The cost of these cyber-attacks not only can result in serious financial consequences for the firm, but to your clients as well.

Insurance firms could face a number of different cyber-attacks:

- Phishing: This attack attempts to steal sensitive information by masquerading as a trustworthy entity. Most commonly your organization will receive an email from what appears to be a trustworthy sender to open a malicious link that will allow the attacker to have access to your system.
- Social Engineering: This is the act of deceiving someone into divulging information that they should not have access to.
- Ransomware: This attack attempts to encrypt files and then demand a ransom payment for the encryption key to unlock those files. These attacks are varied and may have multiply encryptions and they may reach out to your clients as a way to demand additional ransom payments.
- Hacking: This attack can use brute force or exploit weaknesses in your software to get access to user passwords and steal data.

A cyber security policies and procedures manual should be written down and available to all staff members to help protect against cyber-attacks. The manual should identify what data needs to be secured, what threats and risks the firm faces, what safeguards are in place, and what to do in the case of an incident. This manual needs to be reviewed and revised periodically as technological changes occur.

A cyber security manual should address the following:

- Data
  - Inventory, management, and access authority of your firm's resources
  - Backup data
- Safeguards
  - Access/Authorization rights – who has access to what, internal vs external
  - Securing your wireless network
  - Updating your software and systems – including operating systems and anti-virus programs to the latest patches.
  - Early warning systems to detect unauthorized activity
  - Password and encryption standards for all company devices including portable devices
- Risks
  - List the types of cyber-attacks a firm may face and how to identify them
  - Equipment theft, loss, or breakage
  - Third-party services with access to your data
  - Plans for departing employees
  - Employees working from home and social media use
- Incidents
  - Systems in place to monitor for breaches
  - Reporting incidents to consumers, RIBO, and your insurer

Firms can also protect against cyber-attacks by regularly training staff as they are most likely targets of cyber-attacks. Regular security awareness and cybersecurity training programs can mitigate against cyber-attack.

So that they can recognize and respond appropriately to cyber-attacks.

One of the best measures to protect your cybersecurity is to implement Multi-Factor Authentication (MFA) for all employees. MFA requires that employees use two different methods (e.g., phone codes) to verify their identity before they are allowed to log in or gain access to the firm's data. This prevents most phishing and password hacks keeping your data secured. This is a low-cost measure that can save your firm from large claims and reputational lost, and most insurers require MFA to be in place prior to issuing a policy.

CYBER LIABILITY INSURANCE

RIBO also strongly recommends that firms purchase cyber security policies that cover First Party and Third-Party liability coverage and consider sufficient limits to address these exposures. Insurance companies are increasingly requiring brokerages to show proof of cyber liability insurance covering technology and security incidents and errors (including breach of personally identifiable information claims), ommissions/professional liability, communications, and media liability, employee dishonesty and computer fraud.

An example of coverage would include a minimum of $5,000,000 per claim/per occurrence with dedicated Data Breach Response limits. Certain policies may require certain safeguards to be in place which can help round out your cybersecurity policy program.

HELPFUL RESOURCES

The Canadian Insurance Services Regulatory Organizations (CISRO) created a new Cybersecurity Readiness reference tool adapted to insurance intermediaries to which they can refer to in their efforts to prevent cybersecurity incidents and be ready to respond to them should they occur.

https://www.cisro-ocra.com/Documents/View/2582

The Canadian Centre for Cyber Security has produced a number of extensive resources that can help you improve your cyber security:

https://cyber.gc.ca/en

The IBC has developed a helpful resource outlining the threat of cyber-attacks and ways to mitigate that risk:

http://www.ibc.ca/on/business/risk-management/cyber-liability/

FUTURE CONSULTATION

RIBO intends to consult with all licensees as to whether cyber insurance should be a mandatory form of insurance for all registered firms, including Sole Proprietors, Partnerships and Corporations.

Last updated: ______October 25, 2023___