RMA INSURANCE

BULLETIN

March 14, 2024

Upcoming Changes to the Cyber Insurance Requirements

In the face of escalating cyber threats, municipalities are increasingly recognizing the critical importance of cyber insurance. Given the sensitive data and essential infrastructure they handle, municipalities are prime targets for cybercriminals, and successful attacks can result in severe consequences such as data theft, financial losses, service disruptions, and reputational damage. While cyber insurance serves as a valuable resource, it is crucial to understand that it does not replace robust cybersecurity practices.

To underscore the seriousness of this commitment and the imperative of robust risk mitigation, Genesis will implement changes to its cyber coverage **effective November 1, 2024**. Subscribers are required to adopt four crucial cyber risk mitigation tools: multifactor authentication, staff Training, strong Backup Policies, and endpoint detection**.** The adoption of these tools is not only encouraged; **it is essential for sustaining the enhanced coverage.**

Implementing these tools ensures the preservation of the improved coverage. Members who may face challenges in implementing all four safeguards will still benefit from the original limit of $250,000. This shift reinforces the RMA's stance that a comprehensive and proactive approach to cybersecurity is essential for municipalities to safeguard their sensitive data, critical infrastructure, and the trust of their residents against the evolving threat landscape of cyber-attacks.

Multi-Factor Authentication (MFA) / Dual-Factor Authentication (DFA)

To enhance system security, RMA Insurance members will be required to implement Dual-Factor Authentication (DFA) for accessing company accounts and sensitive information. DFA provides an extra layer of protection by requiring staff to verify their identities with something they know (like a password) and something they have (like a mobile app, hardware token, or SMS code). This measure significantly reduces the risk of unauthorized access and data. Detailed guidelines on enabling DFA will be provided upon request, and further is available online.

Staff Training

Human error continues to be a prominent contributor to data breaches. To minimize this risk, it is crucial for all staff members to receive routine cybersecurity awareness training. Such initiatives provide individuals with the means to detect phishing attacks, recognize malware, and adopt best practices for the secure handling of sensitive information. They also encourage vigilance and a proactive approach to identifying and reporting potential threats. RMA Insurance is partnering with the Canadian Internet Registration Authority (CIRA) to provide members with free employee cyber training. CIRA will be providing its Cybersecurity and Awareness training (CAT) platform to members **starting March 2024** to assist in educating employees on the cyber risks in the world today.

Strong Backup Policies

Robust data backup policies are essential for disaster recovery and data protection. RMA Insurance recommends instituting stringent backup policies to ensure the resilience of corporate data in case of a cyber incident or other unforeseen events. Backup policies can include regular offsite and cloud backup of company data amongst others. All qualifying members will be required to comply with these policies to safeguard critical information.

2510 Sparrow Drive Nisku, AB T9E 8N5
Office: 780.955.3639 | Fax: 780.955.3615
RMAinsurance.com

End-Point Detection

Implementing endpoint detection systems is crucial for real-time monitoring and threat exposure. Members' IT staff can deploy endpoint detection solutions on all company devices to identify and respond to suspicious activities. This proactive approach will significantly enhance security posture.

To conclude, members will be obligated to provide proof or documentation of the implementation of each of the four cybersecurity measures upon submission of any cyber claim. Acceptable forms of documentation may include invoices, cyber audit reports demonstrating the presence of these measures within the organization, among others. In the event that members have not yet implemented these measures, they will only be entitled to the standard policy limit of $250,000 against the revised limit at the time of a claim.

In support of cybersecurity practices, Genesis has partnered with CDW (a Canoe approved supplier) and CIRA to provide cyber security tools and employee training. Further details on CIRA and CDW will be communicated to members in the coming weeks, and we encourage members to stay alert for this information. Additionally, members can also use their RiskPro credits to cover expenses that may be incurred while implementing these cyber risk mitigating measures.

For more information on RiskPro credits or anything mentioned in this whitepaper, please contact the RMA risk team at risk@RMAinsurance.com. Keep an eye out for more details on CIRA and CDW in the coming weeks.

Temi Alao
Risk Advisor
587.686.3370
temi@RMAinsurance.com