

Make a List and Check it Twice: Are Your Cyber Programs Naughty or Nice?

Cybersecurity | Litigation | Litigation & Dispute Resolution | Transportation and Logistics

2 January 2026

As 2025 draws to a close, the end of the year offers a valuable opportunity for supply chain intermediaries – including shippers, freight brokers, freight forwarders, warehousemen, and motor carriers – to review and assess the health of their cybersecurity systems, policies, and programs. In today's increasingly digital and interconnected supply chain, the consequences of even small vulnerabilities can have fatal operational, legal, and reputational consequences.

Below, we outline three key cyber and privacy “blind spots” we often see together with practical recommendations on how to strengthen resilience and reduce exposure. Many of these risks do not arise from sophisticated threat actors (of which, there are many), but rather from outdated policies or gaps between written policies and operational / fiscal realities.

The risks set out below are not unique. If you're engaged in the transport or movement of goods along the supply chain either domestically or abroad, there is something on this list for you.

Blind Spot #1: Not Using Multi-Factor Authentication (“MFA”) On All Systems

Multi-Factor Authentication (“MFA”) can be thought of as a sort of “seatbelt” in the privacy and cyber world. In practice, it can represent the last – and sometimes only – line of defence between your organization and a breach. While many organizations have implemented MFA security on their email systems, many of their other critical platforms and servers often remain unprotected. We strongly urge organizations to implement MFA not just on their email servers, but also on programs and platforms used for accounting, billing, payroll, and vendor management. While it may seem like a painstaking process from a practical point of view, the benefits of an organization-wide implementation far outweigh the drawbacks.

Using MFA significantly reduces the risk of accounts or valuable information being compromised and provides an additional authentication barrier which is more difficult for threat actors to bypass.

Given that many identity theft scams, for instance, rely on stolen credentials, properly configured MFA can help ensure that a stolen credential does not in and of itself allow threat actors to gain access to sensitive information.

Blind Spot #2: Not Having Basic Cyber Training or a Documented Incident Response Plan

Routine privacy and cybersecurity awareness and training helps educate employees to recognize phishing and/or other deceptive communication methods which rely on the manipulation of human trust. By regularly training and testing employees to recognize suspicious communications and the patterns associated with social engineering attacks, organizations can mitigate their risk in the face of such attacks.

On a related note, picture the following scenario: You are a C-Suite Executive at a trucking company. Monday morning comes around, and your dispatch systems go down. The phones are ringing with new shipments to move and clients are asking for updates on existing ones. It is then when you receive a ransom note. What's your first move? Who do you call?

Make a List and Check it Twice: Are Your Cyber Programs Naughty or Nice?

The importance of a well planned out, thoughtful, and most importantly practiced Incident Response Plan (“IRP”) cannot be understated. An IRP should be well-documented and reviewed regularly with all those in your organization. It should include a step-by-step protocol for detecting, responding to, and recovering from threat incidents.

An effective IRP must outline the necessary steps and action items necessary to identify and react to a breach incident; evaluate the situation; inform the relevant individuals and organizations about the incident; coordinate the company's response; and assist in the recovery efforts following the incident.

We also encourage organizations to put their IRPs to the test in the form of test breaches. Being well prepared on paper is a virtue, but response plans must be tested (and re-tested). Test breaches are excellent opportunities to test an IRP in a no-risk environment.

Timeliness is a feature which should be the keystone of any IRP. Rapid identification and containment of compromised information and/or accounts are crucial for preventing further unauthorized fraud. Your organization's response should be swift, intelligent, and coordinated.

Blind Spot #3: Overbroad Account Authority & Administrative User Access

Imagine for a moment that you run a trucking company and every single one of your drivers have administrative access to all email, vendor, and financial accounts. Certainly, this would not be a good idea. Cyber criminals understand well that if they can retrieve administrative account credentials, they “get the keys to the kingdom”.

To mitigate this, we strongly urge organizations to adopt the “principle of least privilege”. Limiting user access to the minimum level required to complete the assigned duties reduces the overall available “attack surface” and mitigates the potential impact of credentials in the event they become compromised and fall into the wrong hands.

Conclusion

As we venture into 2026, we urge companies to shift away from annual or one-time reviews of their privacy and cyber programs and move towards a paradigm where the review is an ongoing business imperative. Pro-actively reviewing and identifying risks in policies, programs, communications, data storage, insurance coverage, and internal controls will keep you ahead of the game and can assist your organization in being better prepared and more resilient in the face of threats when – not if – they come. A PDF version is available for download [here](#).

(This blog is provided for educational purposes only, and does not necessarily reflect the views of Gardiner Roberts LLP).

Author



Jamal Rehman



Bay Adelaide Centre — East Tower
22 Adelaide Street West, Suite 3600
Toronto, ON M5H 4E3

Phone: 416.865.6600
Fax: 416.865.6636
contactGR@grllp.com