The makings of great cyber incident response – pre-incident retainers, the role of legal counsel and the first 24 hours

January 31, 2023

More and more, organizations are reaching out to ask about pre-incident retainers – securing us, in advance, to help in the event of a cyber incident. This is a positive and important cyber-readiness step. Here, we provide some background and key considerations.

The role of legal counsel in incident response

Our value goes beyond providing legal opinions. Major cyber incidents are associated with significant business and legal risks – risks that are the regular domain of lawyers. Lawyers who are experienced in incident response can digest limited facts and evidence under pressure, identify how they translate into organizational risk and give clear and decisive advice to help organizations optimize their response. Even in-house teams who are very prepared can benefit from the assistance of experienced outside legal counsel immersed in incident response. Incident response lawyers know the present threat and stakeholder environment, have knowledge of the key stakeholders and issues, and can often provide reliable intelligence. We are careful to respect the line between providing strategic advice (our role) and making decisions (our clients' role), but our clients benefit most from our services when they rely on us broadly, and integrate us into their incident response teams as legal and strategic advisors.

Our large national team has robust incident response capacity. We support our team members through collaboration and knowledge management, and all team members work on incident response files, but also on a wide range of non-urgent work. Therefore, we do not need to charge our clients a fixed fee for being on retainer. Our "retainer" is essentially a promise to respond – immediately – with a qualified team of lawyers led by a partner who will always remain engaged.

The importance of the team

On major incidents, we always work with technical vendors who specialize in remediation, forensics and threat actor interaction and intelligence. Given the

importance of privilege, we are typically asked to assume responsibility for instructing them. To make complicated law simple: if we engage technical advisors to work arm-and-arm with us, the combined advice is arguably all protected as privileged.

Given this arm-and-arm service delivery model, the lawyer-technical advisor relationship must be strong. Organizations who are working up their pre-incident retainers should consider this important point. Retain legal counsel and technical vendors who trust each other and are confident about their ability to work with each other. As legal counsel, we are "vendor agnostic." We nonetheless work regularly with trusted vendors with whom we have honed our joint service delivery though experience. We can adjust to new vendors, especially when a client has a strong preference, but we are often asked to opine on who is good and who might be a best fit for a particular organization.

The first 24 hours

Our clients that approach us about pre-incident retainers are understandably anxious about getting their incident response off the ground. We tell them that the first priority is to prepare containment playbooks and to practice different containment scenarios.

Engaging the vendor team - legal and technical together - comes next. The good news for organizations who pre-retain their vendors is that they will save about six to 12 hours of time that others burn finding and contracting with available vendors. In an incident scenario, pre-retained vendors should still provide a statement of work with a budget estimate, but this will be a much easier document to negotiate than a master services agreement that is entered into in the pre-incident retainer process.

As for who to call first, it doesn't matter! Just make sure you call the whole team. Call all the technical vendors and legal counsel and arrange a scoping call – a chance to convey the basic incident facts and receive preliminary advice. It is ideal that everyone participate, but the vendor responsible for remediation has the leading role out of the gate. Everyone else – legal included – can catch up, and the relationship between counsel and technical vendors is memorialized coming out of the scoping call in any event.

You've retained your team. Now what?

As we have said, written incident response plans (often required by regulators) are a good means of documenting learning and putting information at hand, but ought not to be viewed as the foundation of readiness. Organizations should meet regularly with their counsel and their vendors to discuss and learn. Break down the incident work streams and other aspects of the incident response process and have periodic huddles with the team. Use your counsel and vendors to conduct a tabletop exercise, on at least an annual basis.

Unlike law firms, technical incident response vendors typically charge fixed fee annual retainers to support their response capacity. Most will also allow their clients to recover all or some of this investment by using the retainer to purchase pre-incident services – the facilitation of table top exercises, for example. Organizations should take advantage of such services, but should also involve their legal counsel. The hourly fees will be modest, and the benefit of involving legal counsel will outweigh the cost. Our main point

in this article is that building your outside and inside teams and preparing them to function well together is an essential task.

With that, we will leave you to work on your critical cyber team building and cyber readiness endeavour. We would be pleased to speak with you about it, and about how BLG can work with you and other third-parties so you are ready to perform optimally when confronted with a major cyber incident.

By

Eric S. Charleston, Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.