Bulletin | Cybersecurity, Privacy and Data Protection

June 2021

Cybersecurity incident response – Tips from the trenches

A cybersecurity incident can be challenging and costly for any organization, regardless of size, industry or cyber maturity. Timely advice and guidance from experienced incident response legal counsel can make the process easier and more successful.

Following are some generally applicable practical suggestions, based on real-world experience, for responding to a cybersecurity incident.

- **Hope is not a plan.** Incident response is usually easier, less expensive and more effective if the incident response team has a pre-existing, written incident response plan. In many circumstances, there is a legal requirement to have a suitable incident response plan that is consistent with regulatory guidance and industry best practices. The best incident response plans are short and straightforward, specify practical tasks and achievable outcomes, assign accountability to specific team members, and provide guidance (including communications guidelines) to help the incident response team make risk-based decisions and comply with applicable laws.
- **Preparation is half the victory.** An incident response testing, training and exercise program (including tabletop exercises) can help ensure that an incident response plan is up-to-date and the incident response team and equipment/systems are in a state of readiness, so that the team can respond to cybersecurity incidents in a prompt, effective and lawful manner.
- **Sticker shock (an ounce of prevention).** Incident response costs can be substantial, ransom amounts (if an incident involves ransomware) can be significant, and business disruption losses can be crippling. Wise cybersecurity investments can reduce the risk of incidents and help mitigate resulting losses and liabilities.
- **It's a team sport.** Incident response usually requires a collaborative multi-disciplinary team of internal resources and external consultants/advisors (e.g., supplemental technical personnel, forensic information technology consultants, public relations advisors and experienced legal counsel). Retain external consultants/advisors (including incident response legal counsel) before a cybersecurity incident occurs, so that selection and engagement decisions (including negotiating terms of engagement) can be made in a reasonable manner and consultants/advisors are available and prepared to provide incident response services when required.

- **Are you covered?** As soon as possible, determine whether there is potential insurance coverage for an incident and give written notice to relevant insurers. Cybersecurity insurance can provide priority access to external consultants/advisors. Ensure that incident response decisions (e.g., payment of ransom) are made in accordance with insurance policy requirements.
- **Legal privilege.** Incident response activities should include measures to establish and maintain legal privilege, where appropriate, over incident response communications and documents and help avoid inadvertent and unnecessary disclosures of legal advice.
- **Keep it secret. Keep it safe.** Business email and other communication systems can be compromised by an incident and used by attackers to monitor incident response activities. Incident response teams should communicate using secure out-of-band systems until standard communication systems are determined to be secure.
- **Beware of BYOD.** The use of personal computers/devices during a cybersecurity incident can present technical and legal compliance risks that should be carefully considered. The installation of security solutions (e.g., intrusive end-point detection and remediation software) on an individual's personal computer/device usually requires express consent under privacy laws and *Canada's Anti-Spam Legislation*.
- **Ransomware (back up or pay up).** Ransomware attacks, which often include data exfiltration and extortion, are an increasingly prevalent and serious risk. Access to secure and reasonably current backups is usually necessary to avoid paying a ransom. If making a ransom payment is unavoidable, retain (through legal counsel) a ransomware expert to negotiate with the cybercriminals, conduct appropriate due diligence searches for compliance with terrorist financing and economic sanctions laws, and facilitate the ransom payment.
- **The human factor.** An incident can impose significant stresses on an organization's leadership, personnel (including the incident response team and other employees) and customers. Support the incident response team, and consider the need for additional technical resources (i.e., boots on the ground) to help with containment, eradication and recovery activities. Planning, training and effective communication can help manage stress and reduce the risk of errors.
- **Expect the unexpected.** Be prepared for mistakes and surprises (e.g., failures of incident response technologies, stress-induced errors by the incident response team, and uncharacteristic behaviour by individuals affected by an incident). Address those challenges without distracting from key incident response activities. Surprises and mistakes should be revisited during post-incident (lessons learned) review.
- **Stay ahead of the curve.** Incident response often requires communications to internal and external stakeholders (i.e., employees, shareholders, customers and business partners), including warnings to help avoid or mitigate harm. Incident response communications should be prepared or reviewed by legal counsel to help ensure accuracy, consistency and legal compliance.
- **Reports and notices.** Cybersecurity incidents often trigger legal requirements (both statutory and common/civil law) for reports to regulators (e.g., privacy commissioners) and notices to affected individuals (e.g., employees and customers) and organizations (e.g., customers, service providers, payment card providers and financial institutions). Reports to law enforcement might also be appropriate. Reports and notices should be accurate, consistent and written for all potential readers, including the media and courts. Reports and notices should be prepared or reviewed by legal counsel to help ensure accuracy, consistency and legal compliance.
- **Sharing is caring.** Sharing threat information about an ongoing incident (e.g., through law enforcement, regulators, government agencies, intelligence sharing agreements or ad hoc arrangements) to help other organizations protect themselves is a developing norm that provides collective benefits. Legal counsel can help ensure that information sharing is safe and does not waive legal privilege.
- **Records and evidence.** An incident response team should create and maintain secure and confidential records of the incident and all response activities for use by the team while responding to the incident and for use as evidence in regulatory investigations and legal proceedings. In addition, records of an incident should be created and retained in accordance with applicable statutory requirements (e.g., the requirement to create and retain prescribed records of personal information security breaches imposed by the *Personal Information Protection and Electronic Documents Act*).

- **It's not over till it's over.** Incident response is a fast-paced marathon rather than a sprint. Incident containment, eradication and recovery are only the beginning. Other incident response steps – investigation/assessment, reporting/notification, and post-incident review/lessons learned – are required for legal compliance and recommended risk management best practices.

Cybersecurity incident response can be a high-stakes activity. These tips from the trenches, when combined with the advice of expert technical advisors and experienced incident response legal counsel, can help an organization avoid costly mistakes and achieve incident response success. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Éloïse Gratton
T 416.367.6225
egratton@blg.com

Daniel J. Michaluk
T 416.367.6097
dmichaluk@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.