Bulletin | Cybersecurity, Privacy and Data Protection

March 2023

Ransomware attacks – Tips from the trenches

Ransomware attacks are an increasingly common and serious risk for Canadian organizations of all kinds and sizes. The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2023-2024* warns: "… ransomware is almost certainly the most disruptive form of cybercrime facing Canadians". This bulletin provides practical suggestions, based on real-world experience, for responding to a ransomware attack.

Ransomware attacks

Ransomware is malicious software that prevents access to or use of an infected information technology system or device (an "IT Resource") or related data, and demands (typically through an on-screen ransom note) a ransom for a decryption key to restore the infected IT Resource or data. There are two basic kinds of ransomware – "locker" ransomware (which prevents use of an IT Resource by locking the user interface) and "crypto" ransomware (which encrypts specific files or data so they cannot be used without the required decryption key).

Ransomware is often installed on an IT Resource through fraudulent techniques, such as a deceptive email or text message with a malicious attachment or link (known as "phishing" or "spear-phishing"). Sophisticated ransomware can spread throughout a computer network (including to data stored in cloud services) to install other kinds of malware before the ransomware activates encryption.

A ransomware attack can cause significant economic loss and other harm to the victim organization, including: (1) temporary or permanent loss of data; (2) business disruption loss; (3) costs of restoring infected IT Resources and data (if possible) and otherwise responding to the ransomware attack (e.g., complying with legal reporting/notification obligations); (4) costs and liabilities arising from regulatory investigations and legal claims/proceedings by affected individuals and organizations; and (5) harm to the organization's reputation and relations with customers, employees, stakeholders, and business partners. Ransomware can also cause significant economic loss and harm to the victim organization's customers who depend on the organization's services and products.

Organizations can mitigate the risks of traditional ransomware attacks by creating and maintaining secure and current data backups that can be used to restore affected IT Resources and data without the need to pay a ransom for decryption keys. However, in response to those countermeasures, ransomware criminals have evolved their approach to include "triple-threat" ransom attacks – stealing data before encrypting IT Resources and data and then demanding a ransom payment from the victim organization by threatening to: (1) sell or publish the stolen data on the dark web for use by cybercriminals or the organization's business competitors; (2) use the stolen data to attack or demand ransom from the victim organization's customers, stakeholders, and business partners; and (3) perpetrate additional attacks on the victim organization's IT Resources and internet access.

Canadian and U.S. cybersecurity agencies have issued guidance for preventing and responding to ransomware attacks. For example, see Canadian Centre for Cyber Security's *Ransomware Playbook* and *Ransomware: How to prevent and recover*, Australian Cyber Security Centre's *Ransomware Prevention Guide* and *Ransomware Emergency Response Guide*, U.K. National Cyber Security Centre's *Mitigating Malware and Ransomware Attacks*, and the *U.S. CISA-MS-ISAC Joint Ransomware Guide*. The National Association of Corporate Directors' *2023 Director's Handbook on Cyber-Risk Oversight* provides a list of questions corporate directors should ask senior management to assess their organization's readiness to respond to a ransomware attack.

Law enforcement and cybersecurity agencies have warned that paying a ransom is risky because there is no guarantee that ransomware criminals will keep their promises to deliver effective decryption keys or delete stolen data, and the ransom payment might encourage additional attacks against the victim organization. There are also moral or ethical considerations because paying a ransom will reward and encourage cybercrime, and the ransom might be used to support other criminal activities. Nevertheless, for several reasons, ransomware victims often choose to accept those risks and pay a ransom for decryption keys or data deletion.

Tips from the trenches

Timely advice and guidance from experienced incident response legal counsel can make a ransomware attack response easier and more successful. BLG bulletin *Cybersecurity incident response – Tips from the trenches* provides practical suggestions, based on real-world experience, for responding to cybersecurity incidents, including ransomware attacks. Following are some additional comments and suggestions for responding to a ransomware attack:

- **Starting the clock.** Ransomware criminals often try to create negotiation pressure by starting a negotiation clock when the victim organization responds to a ransom note (e.g., clicks a link in the ransom note) or otherwise contacts the criminals. For that reason, a victim organization should generally not respond to a ransom note or contact the ransomware criminals until the organization has completed initial incident response steps (e.g., engaging legal counsel and technical advisors).
- **Are you covered?** As soon as possible, the victim organization should determine whether it has potential insurance coverage for the ransomware attack, including coverage for ransom payments, and give written notice to relevant insurers.
- **Invoke the incident response plan.** The victim organization should invoke its ransomware attack response plan (including pre-approved guidelines for deciding whether to pay a ransom) and engage its designated incident response team (with applicable insurer approvals).
- **Legal privilege.** Ransomware attack response activities should include measures to establish and maintain legal privilege, where appropriate, over legal advice and related communications (including with external consultants and advisors) about incident response activities and negotiations with the ransomware criminals.
- **Designate a decision-maker.** To help a victim organization make timely and consistent decisions throughout the ransomware attack response, the organization should designate a senior individual with authority to make or coordinate critical risk-based business decisions and instruct technical advisors and legal counsel.
- **Engage a ransomware negotiator/payment facilitator.** A victim organization should engage (through legal counsel) an expert ransomware negotiator to provide threat intelligence and negotiation advice, communicate with the ransomware criminals, conduct clearance searches for compliance with anti-money laundering, terrorist financing and economic sanctions laws (discussed below), and facilitate the ransom payment (if any).
- **Engage a digital forensics incident response firm.** In most circumstances, a victim organization should engage (through legal counsel) an expert digital forensics incident response firm to help with incident response activities, including identifying the ransomware variant, assessing the scope and severity of the ransomware attack (including the duration of the attack and the data accessed and exfiltrated), searching for publicly available decryption keys, and providing technical information and assistance to legal counsel.

- **Information from ransomware criminals.** There are many reasons why a victim organization's forensic consultants might not be able to determine the scope and severity of the ransomware attack (including the data accessed and exfiltrated by the ransomware criminals). In those circumstances, a victim organization might engage with the ransomware criminals, even if the organization has no intention to pay a ransom, to obtain essential information about the ransomware attack (e.g., a list of exfiltrated files and sample proof of exfiltration) the organization can use to make business and legal compliance decisions.
- **Prevent follow-on attacks.** Ransomware criminals might reattack a victim organization (e.g., re-entering the organization's IT Resources using compromised credentials or back-door malware, incident-related email spoofing, or a distributed denial-of-service attack) if the organization refuses to negotiate or pay a ransom or even after a ransom is paid. Consequently, as part of the incident response process, a victim organization should secure its IT Resources and implement measures to protect against and detect follow-on attacks by the ransomware criminals (e.g., searching for malware and other indicators of compromise, implementing email hygiene and endpoint detection and response solutions, resetting credentials, and vigilance warnings to personnel and stakeholders).
- **Validate/test backups and the decryption key.** A victim organization might pay a ransom to obtain a decryption key if the organization does not have viable and reasonably current backups or if the decryption key will help accelerate restoration of IT Resources and data. To make an informed decision, a victim organization should: (1) validate its backups, perform test restorations, and assess data gaps; and (2) validate the decryption key held by the ransomware criminals (e.g., by providing sample encrypted files to the ransomware criminals for free decryption to prove that the decryption key works).
- **Assess stolen data risks.** A victim organization might pay a ransom in exchange for the ransomware criminals' promise to delete and not publish/sell stolen data. To make an informed decision, a victim organization should identify the kinds of stolen data (i.e., regulated personal information, third parties' confidential information, or the organization's own commercially sensitive or proprietary information), the organization's legal obligations and potential liabilities regarding the stolen data, the kinds of harm that might result if the stolen data were published/sold by the ransomware criminals, and the potential business benefits of obtaining the ransomware criminals' data deletion promise.
- **Monitor the dark web.** During the incident response process (and possibly afterwards as well), a victim organization should monitor the ransomware criminals' dark web sites and public information sharing forums for published information about the ransomware attack or the publishing/sale of data stolen from the organization.
- **Payment process.** Ransomware criminals usually demand ransom payments in cryptocurrency to a designated crypto wallet, which might impose additional fees/charges (e.g., costs of buying cryptocurrency) on the victim organization. A victim organization might have to fund a ransom payment even if the payment will be reimbursed under an insurance policy, which might present a cash flow challenge and require senior management or board approval. If a ransom payment might be covered by a victim organization's insurance, the organization should obtain the insurer's written prior approval of the payment to avoid coverage disputes.
- **Legal compliance.** Paying a ransom is not unlawful under Canadian law, provided the payment does not violate proceeds of crime, money laundering, terrorist financing and economic sanctions laws. For those reasons, a victim organization that intends to make a ransom payment should first obtain legal compliance clearance reports (based on searches of the ransomware criminals and their crypto wallet in accordance with regulatory guidance) from qualified service providers. Victim organizations with international operations should verify compliance with all applicable non-Canadian laws.
- **Reports and notices.** Ransomware attacks often trigger legal requirements (statutory, contractual, and common/civil law) for reports to regulators (e.g., privacy commissioners and industry regulators) and notices to affected individuals and organizations (e.g., customers, employees, stakeholders, business partners, payment card providers and financial institutions). Privacy commissioners have expressed the view that a victim organization's payment of ransom for deletion of stolen personal information does not avoid the organization's statutory duty under personal information protection laws to report or give notice that the ransomware criminals stole personal information from the organization. For example, see PIPEDA Findings #2022-004 (Canada), P2018-ND-030 (Alberta), and 07 July 2022 letter (U.K.).

- **Get ahead of the curve.** A victim organization should consider giving proactive notices of a ransomware attack to the organization's customers, employees, stakeholders, business partners and other individuals and organizations before they learn of the incident from the media (based on routine searches of the dark web for information about data security incidents) or they are contacted by the ransomware criminals.
- **Mitigation services for individuals.** Canadian personal information protection laws do not expressly require a victim organization to offer pre-paid credit monitoring/fraud prevention services to individuals affected by a privacy breach (including a ransomware attack). Nevertheless, the Office of the Privacy Commissioner of Canada has explained its view that victim organizations should do so. As a practical matter, in some circumstances offering pre-paid credit monitoring/fraud prevention services to individuals affected by a privacy breach can provide benefits to both the individuals and the victim organization.

Responding to a ransomware attack can be a high-stress, high-stakes event. The comments and suggestions in this bulletin and BLG bulletin *Cybersecurity incident response – Tips from the trenches*, when combined with the advice of expert technical advisors and experienced incident response legal counsel, can help a victim organization avoid costly mistakes and achieve incident response success. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Daniel J. Michaluk
T 416.367.6097
dmichaluk@blg.com

Eric S. Charleston
T 416.367.6566
echarleston@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**.