Bulletin | Cybersecurity, Privacy and Data Protection

February 2021

Cybersecurity Technical Advisory from Five Eyes Cybersecurity Agencies

A comprehensive and regularly tested cybersecurity incident response plan is an essential part of an effective cybersecurity program. In September 2020, the cybersecurity agencies of the Five Eyes nations – Australia, Canada, New Zealand, the United Kingdom and the United States – issued a technical advisory to help organizations pro-actively defend against, and effectively respond to, cybersecurity incidents. The Advisory provides useful guidance for establishing and assessing the technical aspects of a cybersecurity incident response plan.

Cybersecurity Incident Response Plans

The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2020* reports that cybercrime remains the most common threat faced by Canadian organizations of all sizes. A comprehensive and regularly tested cybersecurity incident response plan enables an organization to rapidly respond to cybersecurity incidents in an effective and lawful manner, and is an essential part of a cybersecurity program. In many circumstances, there is a legal requirement – imposed by statute, contract or generally applicable common law or civil law – for an organization to have a suitable incident response plan. Studies (e.g., *Ponemon-IBM Security Cost of a Data Breach Report 2020*) consistently show that a regularly tested incident response plan is the single most effective way to reduce the total cost of a data breach.

An incident response plan should address both the technical and non-technical aspects of incident response. Important non-technical issues include response team organization and operation, legal compliance requirements, legal privilege protocol, internal and external communications, record keeping, evidence collection, notification and information sharing, and lessons learned procedures. An incident response plan should be a living document that is reviewed and revised periodically to reflect changes in circumstances, lessons learned from previous incidents and during testing and training sessions, and evolving legal requirements and best practices.

An incident response plan should be easy to understand and use during a crisis by an incident response team under stress and pressure. It should be a short, simple document that specifies reasonable tasks and achievable outcomes, assigns accountability to specific incident response team members, and helps the incident response team make important technical, business and legal decisions. An incident response plan should be practicable and flexible for use in various scenarios and circumstances, and should recognize the need for incident response team leaders to use reasonable, informed judgment when deciding how to respond to an incident. An incident response plan should include pre-determined but flexible procedures (known as "playbooks") and checklists for various kinds of cybersecurity incidents and guidelines for important decisions.

For more information, see BLG bulletins *Cyber Incident Response Plans – Test, Train and Exercise*, *Data Security Incident Response Plans – Some Practical Suggestions*, *Privacy Breach Response – Prevention of Future Breaches*.

Technical Guidance from Five Eyes Cybersecurity Agencies

Governmental cybersecurity agencies, including the Canadian Center for Cyber Security, are important sources of cybersecurity best practices guidance. In September 2020, the Five Eyes nations' cybersecurity agencies issued *Joint Cybersecurity Advisory: Technical Approaches to Uncovering and Remediating Malicious Activity* to help organizations enhance their cybersecurity incident response by highlighting technical approaches to uncovering malicious activity and recommending mitigation steps according to best practices.

Three Technical Steps

The Advisory sets out three technical steps for responding to a cybersecurity incident:

1. Collect and remove all relevant artifacts, logs and data for further analysis.
2. Implement mitigation steps that avoid tipping off the attacker that they have been discovered.
3. Consider obtaining incident response support from an independent IT security organization with subject matter expertise to help ensure that the incident has been fully detected and resolved and avoid residual issues.

The Advisory describes some technical methods – indicators of compromise search, frequency analysis, pattern analysis and anomaly detection – to discover malicious activity. The Advisory also lists examples of host-based artifacts/information and network-based artifacts/information that should be collected and preserved as part of the first technical step when responding to a cybersecurity incident.

Common Mistakes

The Advisory warns against the following common mistakes during cybersecurity incident response: (1) mitigating affected systems before responders protect and recover data; (2) touching (e.g., pinging and nslookup) the attacker's infrastructure; (3) pre-emptively blocking the attacker's infrastructure; (4) pre-emptive credential resets; (5) failing to preserve or collect log data that could be critical to identifying access to compromised systems; (6) communicating over the same network as the incident response is being conducted; and (7) only fixing the symptoms, not the root cause, of the incident.

Recommended Investigation and Remediation Processes

The Advisory provides the following recommendations and best practices for investigating and remediating cybersecurity incidents from common attack vectors: (1) restrict or discontinue use of ftp and telnet services; (2) restrict or discontinue use of non-approved VPN services; (3) shut down or decommission unused services and systems; (4) cautiously quarantine and reimage compromised hosts; (5) disable unnecessary ports, protocols, and services; (6) restrict or disable interactive login for service accounts; (7) disable unnecessary remote network administration tools; (8) manage unsecure remote desktop services; (9) credential reset and access policy review; and (10) patch vulnerabilities. The Advisory cautions that organizations should tailor mitigations to their specific circumstances. Some of the recommendations could be implemented proactively to prevent or minimize the impact of cybersecurity incidents.

Proactive Defensive Techniques

The Advisory recommends that organizations adopt and implement multiple defensive techniques and programs in a layered mitigation approach known as "defense-in-depth". The Advisory sets out general recommendations and best practices for proactive cyber risk management: (1) user education and training; (2) application allow-listing (also referred to as whitelisting); (3) account control based on the principle of least privilege; (4) regular securely stored backups; (5) workstation management, including asset and patch management; (6) host-based intrusion detection/endpoint detection and response; (7) server management, including asset and patch management; (8) server configuration and logging; (9) change control; (10) network security, including intrusion detection, network traffic monitoring, use of a VPN, strong firewall security and appropriate cloud security (including multi-factor authentication); (11) network infrastructure recommendations; (12) host recommendations; (13) user management, including two-factor authentication and controls for privileged accounts; (14) segregation of networks and functions, including both physical and virtual separation of sensitive information; and (15) additional best practices, including a vulnerability assessment and remediation program, data encryption, an insider threat program, independent security audits and an up-to-date incident response plan.

Comment

The Advisory provides useful best practices guidance regarding some of the technical aspects of a cybersecurity program and a cybersecurity incident response plan. Organizations should consider the Advisory when reviewing and updating their cybersecurity incident response plan. Organizations should be mindful of the limited scope of the Advisory and ensure that non-technical aspects of cybersecurity incident response are adequately addressed in their incident response plan and related testing and training activities. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Cybersecurity, Privacy and Data Protection Group offers comprehensive advice on compliance with privacy laws at the federal and provincial levels as well as with European data protection legislation. We provide both proactive compliance advice and legal advice to help respond to a contravention of privacy laws.

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

© 2021 Borden Ladner Gervais LLP. BD10097–02–21

Borden Ladner Gervais