Cyber Risk Management — PCI DSS Requirements For Incident Response Plan

January 26, 2016

Effective cyber risk management requires a comprehensive plan for rapidly responding to data security incidents.

Effective cyber risk management requires a comprehensive plan for rapidly responding to data security incidents. The Payment Card Industry Data Security Standard ("PCI DSS") specifies basic requirements for an incident response plan, and each payment brand has additional requirements. Most organizations that accept payment card transactions, or store or process payment card data, are contractually required to comply with those requirements or face potentially significant liabilities.

PCI DSS

PCI DSS is a contractual standard, comprised of minimum technical and operational requirements, for the protection of payment card data issued by the major payment brands (e.g. Visa, MasterCard and American Express). Compliance with PCI DSS is required by the contracts governing participation in payment card systems, and applies to merchants who accept payment card transactions and other organizations that store or process payment card data. Failure to comply with PCI DSS can result in serious adverse consequences (e.g. contractual financial assessments and liabilities for resulting financial harm).

Incident Response Plan

PCI DSS requires that an organization implement an incident response plan so that the organization is prepared to respond immediately to a cardholder data security incident, and specifies the following minimum requirements:

- General: The plan must include: (a) roles, responsibilities, and communication and contact strategies for a data security incident, including notification of relevant payment brands; (b) specific incident response procedures; (c) business recovery and continuity procedures; (d) data backup processes; (e) analysis of legal requirements for reporting data security incidents; (f) coverage and responses of all critical system components; and (g) additional procedures required by relevant payment brands. Guidance explains that the plan should be

thorough and contain all the key elements to allow an organization to respond effectively to a data security incident.

- Monitoring/Responding: The plan must include procedures for monitoring and responding to alerts from security monitoring systems. Guidance explains that monitoring systems that focus on potential data risks are critical in taking quick action to prevent a breach and must be included in incident response processes.
- Personnel: The plan must be disseminated, read and understood by properly trained personnel, and designated personnel must be available on a 24/7 basis to respond to alerts of possible data security incidents. Guidance explains that untrained personnel can exacerbate a data security incident and hinder a post-incident investigation.
- Testing: The plan must be tested at least annually, including by reviewing the plan, examining related procedures and interviewing personnel, to verify that the organization is prepared to respond immediately to a data security incident and that the plan and related procedures were followed for previously reported incidents.
- Continuous Improvement: There must be a process to modify and evolve the plan according to lessons learned after each data security incident, and to incorporate industry developments, so that the plan is current and capable of handling emerging threats and security trends.

Payment Brand Requirements

In addition to PCI DSS requirements, each payment card brand has its own detailed, specific requirements for responding to an actual or reasonably suspected data security incident. Those requirements include specific notice and reporting obligations, cooperation with investigations by one of the payment brand's designated assessors and other time-specific procedures.

Comment

A comprehensive, practiced and tested incident response plan is essential for a timely, effective response to a data security incident. The basic requirements for incident response plans imposed by PCI DSS do not include important technical detail and do not identify fundamental legal considerations relevant to incident response planning and preparation, such as legal compliance considerations, procedures to collect and preserve admissible evidence and practices for properly protecting privileged communications. Organizations should obtain appropriate technical and legal advice when preparing an incident response plan.

By

Bradley Freedman

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 725 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