haynesboone

Haynes and Boone, LLP

A Desk Guide to Data Protection and Breach Response

haynesboone.com

Austin Chicago Dallas Denver Fort Worth Houston
London Mexico City New York Orange County Palo Alto
Richardson San Antonio Shanghai Washington, D.C.

haynesboone

For additional information, please contact:

RONALD W. BREAUX
Privacy and Data Breach Practice Group Leader
ron.breaux@haynesboone.com
T +1 214.651.5688

haynesboone

haynesboone

A Desk Guide to Data Protection and Breach Response

Foreword

If your business is connected to the Internet, it is vulnerable to attack, either by willful perpetrators intent on exfiltrating your proprietary or sensitive data for their own personal gain, or by casual hackers or hacktivists intending to cause damage to your business. Unfortunately, companies should prepare for "when" – not "if" – they suffer a data breach. In fact, the chances are good that your business has already suffered an attack. Attacks come in a variety of forms, from viruses to spam, from Trojan Horses to network backdoors and other nefarious technology, all of which can be used to wreak havoc on your business in a variety of ways. Indeed, data breaches – and the resulting loss of critical data, business interruption, onerous disclosure requirements, regulatory scrutiny, costly third party litigation, and tremendous loss of reputation and goodwill – can threaten the very viability of your enterprise.

Haynes and Boone is pleased to present this "Desk Guide to Data Protection and Breach Response" to help you navigate the rapidly evolving cybersecurity landscape. The Desk Guide, which was prepared by the firm's interdisciplinary Privacy and Data Breach group, provides a practical approach to data security, including how to:

- identify and analyze applicable data protection and compliance issues,
- develop an enterprise data security plan,
- obtain cyber risk insurance,
- investigate and respond to a breach or cyber incident,
- address public disclosure and regulatory issues following a breach,
- refer cyber incidents to law enforcement for possible investigation and prosecution,
- anticipate and prepare for civil litigation and class actions following a data breach or cyber incident, and
- recover losses through insurance claims.

We hope this Desk Guide will be a useful reference for you as you manage your company's cyber risks and prepare for the cyber incident(s) your company will almost certainly experience. If you have any questions about the Desk Guide or about privacy, data security or data breach matters more generally, please contact any of the members of our Privacy and Data Breach group. We look forward to working with you.

The Best Defense is a Good Game Plan: A Proactive Approach to Data Protection and Compliance

Ronald W. Breaux, Emily Westridge Black, Gavin D. George, Timothy Newman

In our experience, the best defense against potential data breaches, investigations by privacy regulators, customer privacy complaints, and mishandling of sensitive data by vendors is a well-constructed and well-monitored privacy compliance and data protection plan. In this first installment of our series, we will discuss the initial steps companies should take to create an effective privacy compliance and data protection plan.

Assess Your Data Retention

Before beginning to design a data protection plan, your company should identify the types of information it collects and processes. Under current laws and regulations, the following types of commonly collected information require special handling and protection:

- Personal Information ("Personally Identifiable Information" or "PII") – State data breach laws define personal information generally to include an individual's first name or first initial and last name in combination with any one, or more, of the following identifiers: social security number; drivers' license number or state identification card number; account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. Many states add additional elements to this definition, including medical data, passport numbers, or tax identification numbers. Some states, including California, also include personal email addresses in the definition, when accompanied by a password or security question and answer.
- Cardholder Data – The Payment Card Industry Data Security Standard ("PCI DSS") defines cardholder data as: "account number, cardholder name, expiration date, and service code." The term also includes more sensitive data used for authentication of transactions (PIN, security code).
- Personal Health Information ("PHI") – Generally speaking, the federal Health Insurance Portability and Accountability Act ("HIPAA") defines protected health information to include data about health status or health care linked with certain personal identifiers. These identifiers include, among other things, name, geographic location (more specific than state-level), dates, phone/fax numbers, email addresses, and social security numbers.

  Additionally, apart from information linked to an individual, companies often store business and technical information that they consider confidential or secret, and would prefer to keep from competitors and the public.

Also available as part of the eCourse
[Preventing, Detecting, and Responding to a Data Breach: Internal Controls and Compliance]

First appeared as part of the conference materials for the
2017 Essential Cybersecurity Law session
"Incident Response and Breach Disclosure"