NEAL GERBER EISENBERG

Record-Setting Target Settlement Changes Expectations for Institutional Data Security

June 5, 2017

On May 24, 47 state attorneys general settled with Target for $18.5 million regarding its 2013 data breach. The implications of the agreement may be more far-reaching than many companies realize. The fact that nearly all attorneys general united their efforts to obtain the settlement implies that most states view the new standards set for Target as a framework for data security best practices going forward. The changes in policies and procedures for Target will likely become the *de facto* guidelines for businesses wishing to avoid regulatory action in the wake of a data breach.

The facts underlying Target's breach appear to drive many of the settlement requirements. Instead of accessing Target's gateway server directly through the retailer, cyberthieves gained access using credentials illegally obtained through a third-party HVAC vendor. The hackers then uploaded malware to steal customer data. Although Target's security software sounded alarms as it recognized the malware, Target decision makers decided that no immediate action was warranted. Ultimately, the breach compromised the data of more than 70 million customers.

The ramifications of Target's breach have been significant. In March 2014, Beth M. Jacob, Target's most senior technology executive, resigned. Following the breach, Target reportedly has incurred more than $200 million in various breach-related costs, including legal fees, and likely will spend an additional $10 million to settle a consumer class action. Perhaps more significantly, Target agreed to adopt advanced technical security procedures and complex administrative measures to rectify their vulnerabilities and prevent further breaches, including the following:

- Implement a data security program including:
  - Segmenting cardholder/customer data from the rest of the computer network
  - Implementing password rotation and strength policies
  - Instituting two-factor authentication
  - Implementing access control and management
  - Monitoring file integrity
  - Whitelisting
  - Maintaining logs of network activity
  - Change controls
  - Adopting payment card security technologies (including encryption to protect data or to disable access to such data remotely in the event it is compromised).
- Audit contractors and subcontractors for compliance with security programs.
- Hire an executive to manage/oversee the security program.
- Employ a qualified, independent third-party contractor to thoroughly and properly assess cybersecurity.

Some organizations, and particularly those with limited resources, may find aspects of the above measures challenging to implement either from a technical or a budgetary perspective. However, all entities that manage, process, maintain, or are otherwise involved in the transmission of consumer, client, or employee data should carefully consider the roadmap set forth in the Target settlement, and seek assistance to revisit their existing security policies and procedures, to implement new practices to best position themselves to avoid data breaches in the first instance, and to weather the storm if a security incident does occur.

DATA SECURITY

NEAL GERBER EISENBERG

The Target example underscores that having robust security software infrastructure alone is not enough to protect an organization. A holistic approach to security embracing technological, administrative and physical safeguards, together with strong policies and decision-making, is required within an organization to minimize the likelihood of a security event in the first instance and to respond swiftly and fulsomely if and when a breach occurs. To that end, a properly written and well-rehearsed data breach response plan provides key decision makers a protocol to help mitigate the severity and impact of future data breaches. The landscape has changed, and institutions will need to learn from Target's experience and adapt accordingly.

• • • • • • • • • • •

Neal Gerber Eisenberg's Information Governance Consulting professionals regularly help clients design, draft, refine and implement the full suite of internal policies necessary to support an IG (information governance) program, including policies, written information security policies, data maps, BYOD (bring your own device) policies, and data breach response plans. They also can provide assistance in assessing or auditing already-existing plans. For assistance, more information, or a free consultation, please contact Neal Gerber Eisenberg partners Greg Leighton (312.269.5372, gleighton@nge.com) or Sarah Smith (312.269.5257, ssmith@nge.com).

DATA SECURITY

• • • • • • • • • • •