THOMPSON HINE

Privacy & Cybersecurity Update

December 2020

Responding to the SolarWinds Breach: Compliance and Oversight Considerations

Several media outlets recently reported on a sophisticated cyber operation that targeted a SolarWinds Orion network management product, which ultimately enabled the perpetrator to clandestinely access the information technology (IT) environments of several U.S. government agencies and thousands of private-sector organizations. In response, businesses have scrambled to both implement appropriate security protocols to mitigate their exposure and risk and investigate whether their (direct or indirect) use of SolarWinds Orion constitutes a data "breach" requiring formal disclosure to a third party or regulatory agency. As part of its investigatory efforts, a business should consider a broad range of potentially applicable legal requirements and best practices, such as protecting investigation and remediation activities under the attorney-client privilege, developing and retaining compliance documentation and records, and managing or overseeing its service provider's response to the breach.

The SolarWinds Orion Breach

SolarWinds Orion is an IT solution that provides an end user the ability to monitor, manage and analyze the performance and operability of its computer system and network. Given its core functionality, this solution is often installed on an organization's most mission-critical infrastructure. In March 2020, a foreign nation-state (possibly Russia) unlawfully accessed the internal systems SolarWinds uses to develop updates and upgrades to the Orion product line and inserted malicious code in the underlying software. In turn, organizations that initiated updates to their Orion products (after this compromise in March) unknowingly installed malware in their own IT environments. The malware included a "Trojan" program designed to take control of systems and networks and secretly communicate with a remote server operated by the foreign nation – but only after remaining dormant for several days or weeks to avoid detection. Once fully compromised, the foreign nation could systematically control a compromised device and access data stored on it.

Incident Response Considerations

Since the reports of the SolarWinds Orion breach surfaced, organizations have been investigating whether their use of this solution has resulted in a "breach" that requires formal disclosure pursuant to a data breach notification law. It is imperative for an organization to ensure that it undertakes its investigatory efforts in the context of its broader legal requirements and in accordance with data incident response best practices. However, the following legal, procedural and oversight obligations and considerations are at risk of being overlooked, given both the unique nature of the SolarWinds attack and the pace at which technical remediation has already begun.

Incident Response and Legal Privilege

Many businesses have addressed ransomware, phishing attacks and other malicious cyber operations, as these are, unfortunately, common occurrences across industries and jurisdictions. It is a best practice, and in some instances a legal requirement, for an organization to develop and maintain a data security incident response plan to assist in identifying and responding to such incidents. A key part of any data incident response program is having a qualified attorney strategically lead an investigation of the incident to

ensure the business is well-positioned to defend against reasonably foreseeable litigation. This includes asserting legal and evidentiary privileges over communications conveyed and analysis produced during the investigation. Accordingly, following a data incident, it is the responsibility of counsel (preferably outside counsel) to:

- define the scope of the investigation,
- retain independent cybersecurity and forensic experts,
- instruct both internal employees and outside consultants on their responsibilities,
- issue litigation holds, and
- render advice regarding the organization's legal obligations.

Although the tactics used in the SolarWinds breach are not as common as other cybersecurity attacks (e.g., ransomware, phishing), an organization should still adhere to these core data incident response principles and processes as it implements its technical remedial measures. This is especially important given the uncertainties still surrounding the SolarWinds breach and the fact that discovery and privilege issues are closely scrutinized during data breach-related litigation.

Compliance Documentation

Several federal and state legal obligations mandate that an organization draft and retain records pertaining to its investigation of a data security incident, which apply even when the underlying incident does not rise to the level of a data "breach" requiring formal disclosure pursuant to an applicable data breach notification law or regulation. For instance, federal laws and regulations that apply to healthcare providers and employee benefit plans require organizations to document and retain records pertaining to a "security incident," which is defined more expansively than a "security breach." In addition, certain state data breach notification laws require organizations to develop and retain documentation pertaining to their investigations of security incidents, which is especially important when an organization determines (after concluding such an investigation) that it is not legally required to publicly disclose an incident to a third party or regulatory authority.

Accordingly, it will be important for an organization to understand and enforce applicable compliance documentation and records retention obligations as part of its investigation into whether the SolarWinds breach impacted its operations. If such legal obligations are not applicable, the organization should consider following guidance set forth by the National Institute of Standards and Technology describing how organizations can implement systems to track and document security incidents.

Managing Service Providers

It is common for businesses to rely on third-party service providers to maintain and operate their IT infrastructure and to retain confidential, proprietary and other sensitive data on their behalf. Due to the nature of their data services, such third parties may be subject to legal and contractual obligations that have been implicated by the SolarWinds Orion breach. For instance, many states have enacted laws requiring service providers to agree to specific contractual obligations pertaining to data security and to notify clients for whom they are processing data in the event of a data breach or incident. The federal government has issued similar laws that are applicable to organizations operating in certain regulated industries (e.g., healthcare, financial services, defense). Often these contracting requirements are manifested in master services agreements and other contractual provisions requiring a service provider to inform its client of a data incident that compromises the confidentiality, integrity or availability of the client's business data. Yet it is also common for such contracts to require a service provider to notify its client of any incident that materially impacts the security, operability or functionality of its IT environment, regardless of whether the client's specific business data was compromised.

Accordingly, businesses subject to these requirements should expect their data service providers to furnish them notice on whether and to what extent the SolarWinds Orion breach impacted their data processing operations. Alternatively, businesses should consider proactively requesting that their third-party service providers inform them of their current cybersecurity posture, including whether they employed SolarWinds Orion and, if so, whether they have addressed the vulnerabilities therein.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Mona Adabi
202.263.4147
Mona.Adabi@ThompsonHine.com

Darcy M. Brosky
216.566.5774
Darcy.Brosky@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

or any member of our Privacy & Cybersecurity group.