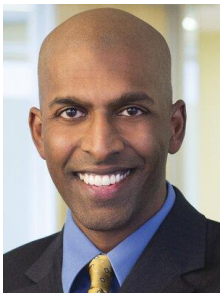
5 Lessons For SaaS Companies After Blackbaud Data Breach

By **Aravind Swaminathan, Joseph Santiesteban and Hannah Levin** (February 22, 2024)



Aravind Swaminathan

Joseph Santiesteban

Hannah Levin

Protecting the brand and mitigating legal risk from a cybersecurity incident is difficult for any organization, but for software-as-a-service businesses, the task is particularly complex.

In addition to navigating more than 50 potential state notice laws and regulations, contractual requirements, complex federal regulatory requirements and new U.S. Securities and Exchange Commission disclosure requirements for public companies, SaaS companies face pressure to satisfy customer needs while managing relationships with customers.

They also must navigate particularly thorny legal, logistical and reputational challenges around what information to share, who is going to make required individual and regulator notices and how — unsurprisingly for SaaS businesses — to do all of this at scale. Regulators have increasingly scrutinized how SaaS companies solve these problems, insisting they prepare and execute decisions quickly after a data breach.

In the past year, Blackbaud Inc., a SaaS provider of education and nonprofit software, resolved enforcement actions with the SEC in March,[1] state attorneys general in October,[2] and most recently the Federal Trade Commission at the start of February[3] relating to a ransomware attack they suffered in 2020. The incident, Blackbaud's response and the resolutions from these matters provide important lessons to help SaaS companies manage these increasingly common forms of data breaches.

Blackbaud Case Study

Background

In May 2020, Blackbaud identified a ransomware attack resulting in the theft of millions of records of personal information Blackbaud stored for thousands of education and nonprofit customers.

After conducting an "exceedingly inadequate investigation," regulators say, Blackbaud told its business customers in July 2020 that consumer personal and financial data had not been accessed. Blackbaud said the same thing in a Form 10-Q filed with the SEC.

The business customer communication stated, "No action is required on your end because no personal information about your constituents was accessed."

Later that month, though, further investigation allegedly revealed personal information had been compromised, but Blackbaud omitted this information from a subsequent 10-Q filing. It did not update customers until October.

Enforcement Resolution

In the aftermath of the breach, Blackbaud resolved a series of enforcement actions from the FTC, SEC and nearly every state attorney general. While not binding on other companies, these resolution agreements shed light on regulatory expectations for SaaS data breaches.

Blackbaud reached agreements with state attorneys general and the FTC to:

- Pay $49.5 million and enter in two consent orders regarding cyber and breach response practices;

- Specify in new contracts the roles and responsibilities for the company and its customers with respect to individual breach notifications;

- Develop an incident response plan and perform tabletop exercises on the plan; and

- Notify the FTC within 10 days of any breach notification to federal, state or local law enforcement;

Blackbaud also reached an agreement with the SEC to pay $3 million and refrain from further violating securities laws, which would include implementing disclosure controls and procedures the SEC alleged were missing.

Blackbaud also agreed to take certain steps in the event of a data breach:

- Offer customers reasonable guidance, cooperation and assistance to determine whether and which data was affected by the breach, including offering guidance on how to use the Blackbaud app to do so;

- Run required queries and reports for customers who are unable to use the app to identify affected data; and

- Provide customers with information to execute required individual or regulator notices, including helping customers determine the identity of affected individuals.

5 Things SaaS Companies Should Consider Doing

1. Prepare a strategy for mass notifications resulting from an incident.

Consider whether you or your customers will notify regulators and individuals. There are pros and cons to either approach, but for larger incidents, it is common for the breached entity to provide many of these notices on behalf of its customers.

This can give the breached entity more control over the messaging and allows it to benefit from economies of scale for notices and credit monitoring services. The answer here will vary depending on the incident, but planning ahead and being thoughtful about potential scenarios can help a company move quickly after an incident.

2. Plan the logistics for mass customer and consumer notices.

When planning notification to customers, align on who to contact and how. Many SaaS companies have lots of contacts for customers, and there is not always a clear primary contact for a data breach. Similarly, there are often options for how to communicate, including email, in-app messaging or a blog.

Also, plan for a secure and effective method to communicate and share data, so customers can analyze their legal requirements. And finally, familiarize yourself with your contractual provisions. Having a good understanding of what you agreed to do is critical.

3. Assign decision makers and execution responsibilities.

No matter how much a business prepares, it will need to make decisions quickly and with imperfect information. Assign these responsibilities before an incident. Effective execution requires collaboration among internal and external teams from security, legal, public relations, customer support and sales. Understand the roles and responsibilities of each and build relationships before an incident occurs.

4. Communicate accurately, transparently and in a timely manner.

When an incident happens, there can be immense pressure to communicate, including updates that may be aspirational. The reality is that these investigations take time, and it is often most important to demonstrate you understand the gravity of the situation, have dedicated needed resources and are taking steps to contain, investigate, remediate and communicate.

Publishing inaccurate information can undermine trust and significantly increase legal liability. Once the facts are known, communicate the information customers will need to perform their own legal analysis.

5. Develop cyber-specific disclosure controls.

A trend in SEC enforcement actions, including in Blackbaud, is that important technical details from an investigation are not escalated to management for disclosure evaluation. To avoid this, plan ahead of time which kinds of incidents to escalate to legal and management, and plan to provide them with the information necessary to make disclosure decisions.

The Bottom Line

Following these steps can help SaaS companies mitigate legal and reputational risk and comply with a dizzying array of state and federal rules and regulations related to cybersecurity and data privacy. It's an increasingly important business imperative in a world where data breaches represent a growing challenge for SaaS companies.

Aravind Swaminathan and Joseph Santiesteban are partners, and Hannah Levin is an associate, at Orrick Herrington & Sutcliffe LLP.

Associate Cosmas Robless contributed to this article.

[1] Press Release, SEC, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48.

[2] Press Release, New York State Office of the Attorney General, Attorney General James and Multistate Coalition Secure $49.5 Million from Cloud Company for Data Breach (Oct. 5, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-495-million-cloud-company.

[3] Press Release, FTC, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax.