Client Alert: Five Ways to Spruce Up Your Company's Incident Response Plan

CLIENT ALERT | 5.22.2017

Each year, companies subject to the Payment Card Industry Data Security Standard (PCI-DSS) must review and update their incident response plans to ensure they are in proper compliance. Additionally, even for companies not subject to PCI DSS, having an incident response plan in place is recommended, as it will greatly assist in investigating and responding to suspected or actual cyber-attacks and data breaches. Cyber insurers, your company's primary regulator, and boards may also require that a company develop and regularly updates its incident response plan.

Now that spring (and the second quarter of the year) has sprung, consider updating your incident response plan for 2017. While making sure your organization's response plan is updated may seem like a large task, there are five actions you can take to accomplish this goal well before the year's end.

1. **Schedule a Tabletop Exercise**. Calendars of key stakeholders fill up quickly, and now that spring break has passed for many, business partners are scheduling meetings and summer vacations. Go ahead and set a date for a tabletop exercise this year, which may be in the third quarter or even the fourth, to make sure everyone who needs to participate can and to avoid scheduling conflicts. The benefits of these exercises are many, including effectively reviewing your plan and discovering and working out any gaps in your plan. Additionally, these exercises are typically a modest commitment in terms of time, costs and resources, encourage team building, and are a good way to familiarize key stakeholders with their roles and responsibilities. If your organization is subject to PCI-DSS, setting and conducting the tabletop will satisfy the requirement to annually test your incident response plan.
2. **Identify Law Enforcement Contacts.** Identify the law enforcement contacts that your organization would notify in the event of a cyber-attack or breach. Include their reporting requirements (such as a 1-800 number or web form) and contact information in your plan for ease of reference. Additionally, many agencies will establish working relationships ahead of time and are willing to partner with you to educate you and your team about how they may be able to assist your company in the event of a suspected cyber-attack or breach
3. **Review Your Cyber Insurance Coverage**. Review your cyber insurance coverage for key terms in the event of an attack or breach, such as how quickly your must notify your cyber insurer to claim coverage and your deductible amount. Your policy may also cover proactive steps and costs such as tabletop exercises, and may be able to assist you in approving certain breach related vendors and costs ahead of time. Additionally, the organization should evaluate its current risk exposure based on the risks it faces and the information it currently has, and reevaluate your coverage with the current risk exposure in mind. If your organization does not have cyber insurance, now may be a good time to consider obtaining it.

4. **Make Sure Legal Obligations Are Updated**. New Mexico recently became the 48th state to enact a notice of breach law, and several states, including Illinois, Tennessee and Rhode Island amended their notice of breach laws last year. Additionally, the Federal Trade Commission and the National Institute of Standards and Technology released guides for managing suspected or actual data breach events. Review your plan to make sure that the latest legal requirements, regulator guidance and industry guidance are incorporated where appropriate. Your outside legal counsel can assist with these review efforts, if you do not have a dedicated in-house privacy counsel.
5. **Review Privilege Protocols**. In the past year, several courts have upheld the attorney-client privilege protecting breach-related reports and documents created as part of the investigation, which can be beneficial to your organization. In-house counsel have a key role in leading or participating in the investigation in conjunction with outside counsel, and educating their clients on the limits of the privilege. Make sure that all key stakeholders are educated on the benefits and limits of the attorney-client privilege, and how to keep privilege intact during an investigation.

Updating your incident response plan is important and can help protect your company in the event of a suspected cyber-attack or breach. For questions about the law, please contact Heather Enlow-Novitsky, or your Vorys attorney.