Cybersecurity Awareness Month – Quick Tips to Effectively Prevent, Prepare for and Navigate a Data Breach

Cybersecurity Awareness Month serves as a great reminder that all organizations should continue to prevent and prepare for a data breach. With the increased risk of cybersecurity incidents or data breaches, keeping up with the rapidly evolving cybersecurity world is important. A data breach is one of the most significant risks for organizations in 2022 and will continue to be for the foreseeable future. Below we have outlined some quick tips to effectively prevent, prepare for and navigate a data breach.

1. Strike a balance between prevention and planning.

A failure to develop and implement an Incident Response Plan (IRP) can prove to be just as disastrous as a failure to implement appropriate security measures to prevent a breach. Striking a balance between prevention and planning can help limit legal exposure on both the front-end and back-end of a data breach.

2. Make sure your IRP can be easily and quickly implemented in the event of an incident.

In order for an IRP to be effective, it is important that all necessary parties, including third-party vendors and outside counsel, are identified and prepared to respond immediately in the event of a cyber incident. The IRP should be flexible and act as a guide for all necessary parties, rather than as a rigid set of rules. One way in which organizations can test their IRP and team is by running a cybersecurity tabletop exercise.

3. Be Responsive!

A cybersecurity incident could lead to litigation or governmental enforcement action. As soon as an organization becomes aware of a potential data breach, it should contact its information technology team, legal counsel and cybersecurity insurance carrier. Organizations should also take steps to investigate the incident and to preserve evidence and other information. Forensic experts may be necessary to assist with the investigation and preservation process. Legal counsel may be necessary to advise of any reporting obligations that may be legally required based on the nature of your business or data breach. Organizations should be weary of disclosing facts relating to the breach other than required reporting obligations and notices, as public statements may be used against you in litigation or enforcement actions. It may make sense to coordinate your response with a public relations team.

4. Keep Up to Date!

Cyber criminals and threat actors continue to evolve and learn. Making sure your organization's information technology team and/or infrastructure is staying up to date is imperative to preventing a data breach. This includes implementing regular offline backups, utilizing encryption technology and endpoint detection, installing the latest updates and having access controls like multi-factor authentication. Certain state and federal laws, rules and regulations now require businesses to maintain adequate safeguards.

Organizations should also ensure that their outside vendors are also maintaining appropriate physical, technical and administrative safeguards, which can be accomplished through contractual provisions, audits, or through the request for proposal process for new vendors.

Further, one of the most important prevention and preparation steps an organization can take is to ensure that its employees, contractors and other third parties are receiving regular security training. A few of the most important aspects of effective incident response are prevention and early detection, which means your preparations may need to include training concerning phishing, recognizing security events quickly and reporting to appropriate individuals.

Organizations should also review their policies and procedures at least annually to ensure that they are up to date and reflect best practices, updated technology standards, new legal requirements as well as changes to organization structure.

5. Don't be dismissive of the risks.

The fact that headlines are dominated by large-scale data breaches makes it easy to forget that small organizations fall victim to cyber events every day. It is important to acquire and maintain adequate cybersecurity insurance to cover these risks. Any organization, large or small, should take appropriate steps to prevent and prepare for a data breach.

For more information regarding Data Breach preparation and response, contact Amber Lawyer, CIPP/E, Shannon Knapp, CIPP/US or any attorney in the cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Jared Joyce for assisting with researching and drafting this memorandum.*

BOND SCHOENECK & KING ATTORNEYS