Is Your Organization Prepared for a Data Breach?

Data breaches are on the rise with **2023 setting a new record all-time high**. There are many different types of data breaches, including those caused by cyber criminals using ransomware, by rogue employees stealing company data, or by human error resulting in unauthorized access to data. Regardless of the cause, data breaches can cause significant consequences for the organizations they affect, including disruption to business operations, financial losses,

reputational harm, loss of sensitive and valuable data, and a multitude of legal implications. They can also have serious implications for affected consumers, who may have their identity stolen or financial accounts hacked. For example, a Maryland health care organization was **recently in the news regarding class action lawsuits filed following a data breach**.

Given the increased frequency in data breaches and the significant risks they present, it is important to evaluate whether your organization has a strong data breach response plan in place. Data breach response plans can help your organization react swiftly and effectively to mitigate risks posed by a data privacy or security incident.

A data breach response plan should include a number of key steps, including:

1. **Notify with your organization's breach response team.** Ensure all team members understand the incident and are prepared to take action to carry out their role within the breach response plan. Maintain open communication channels among team members so everyone remains informed.

2. **Immediately act to stop any active threat and secure your organization's data and information systems.** The actions required to accomplish this will vary depending on the nature of the breach and the information systems and actors involved. IT experts and forensic investigators may be needed to determine the cause and scope of the breach, and to help find a solution to patch vulnerabilities and prevent a recurrence.

3. **Promptly report the incident to your cyber insurer.** Cyber policies vary in scope and your cyber insurer will determine if your policy provides coverage for a particular incident. If the incident is covered by your policy, your cyber insurer will typically launch an investigation and provide legal and forensic experts and other resources to help manage the data breach response.

4. **Contact law enforcement.** If the data incident involves an active, past, or threatened cyber incident, report to local and federal law enforcement authorities **in accordance with their reporting guidelines**.

5. **Determine your legal requirements.** All states have enacted legislation requiring notice to consumers of security breaches involving certain personal information. Organizations may also be subject to other state and federal breach notice laws and response requirements depending on their industry and other factors. Consult with legal counsel to determine whether the incident is considered a "breach" under applicable state and federal privacy laws, which may require notice to affected consumers, regulators, law enforcement, and the media.

***The above list is by no means exhaustive, but intended to encourage reflection of key considerations and the value that a comprehensive data breach response plan can have in saving precious time and resources. Every minute counts when cyber criminals can use that time to access additional sensitive data or disrupt your organization's operations.*

What actions should your organization consider to prepare for a potential breach?

- **Review your data breach response plan:** Ensure your organization has adopted a data breach response plan and review it regularly to ensure it

provides a comprehensive response plan. There are helpful data breach response plan guides available from a number of federal agencies and other organizations such as the **FTC**, **Office of Information Security**, and the **U.S. Department of Education**.

- **Provide training:** Provide training to team members with roles in the data breach response plan. Provide privacy and security training to all applicable members of your organization.
- **Review cyber insurance policy:** Evaluate your organization's cyber insurance policy to ensure adequate coverage is available.
- **Update risk assessment:** An ounce of prevention is worth a pound of cure. Maintaining and regularly updating your organization's privacy and security data risk assessment and acting on key risks can help prevent breaches.

**This client alert is for informational purposes and is not legal advice. View previous issues of Monday Minute.*

For more information on how to help your organization proactively approach a potential data breach, please contact your Gallagher attorneys:

Mallory Regenbogen

Alison Best Lutich

Recent Case Studies

"Why We Do What We Do: Asylum Case Victory is Meaningful to Gallagher Team"

About Our Firm

For more than 60 years, Gallagher Evelius & Jones has served as trusted counsel to businesses including real estate developers, regional and local healthcare systems (nonprofit), religious entities, universities and colleges, clean energy investors, and more, building longstanding relationships with organizations across the Mid-Atlantic region and beyond. Our attorneys focus on the practice areas important to our clients including litigation, employment, tax, finance, real estate, and general corporate matters.

Gallagher and its more than 100 staff are committed to supporting the community through volunteer and pro bono efforts, and to focusing on diversity, equity, and inclusion across all

aspects of the organization.

Share This Email

Join Our Mailing List

Gallagher Evelius & Jones | 218 North Charles Street, Suite 400 | Baltimore, MD 21201 US

Unsubscribe | Update Profile | Constant Contact Data Notice

Constant Contact

Try email marketing for free today!