PRIVACY & CYBERSECURITY

Data Breach Response Checklist

Michael Best

Cybersecurity threats are a growing challenge. In the last few years, we have witnessed a precipitous increase in the number of cyber intrusions in the private and public sector. For most organizations, it is virtually impossible to predict when or how a cybersecurity incident will occur. A single data breach could prove catastrophic, so organizations must be prepared to respond quickly and effectively to prevent further data loss, minimize operational disruptions, and reduce their exposure to legal and regulatory actions.

The Michael Best Data Breach Response Checklist includes specific actions to help organizations tackle the complexity of today's complex cybersecurity threat landscape and improve their cybersecurity preparedness.

How We Can Help

The Michael Best Privacy and Cybersecurity team possesses deep knowledge and extensive experience in helping organizations minimize the threat of security compromises and data breaches by developing strategies to mitigate their risk. We also assist in planning for cyber incidents, effectively responding to data breaches in the earliest phases, and providing counsel on the legal and policy issues that may arise when sharing cyber threat information. Please feel free to reach out to Michael Best's Privacy and Cybersecurity attorneys for questions or assistance.

Preventative Measures

- Establish and maintain a written data breach response plan.
- Identify the key members of your organization's incident response team and the appropriate incident handling procedures.
- Identify key information systems where personally identifiable information (PII) and sensitive data is stored.
- Employ automated tools to monitor and quickly detect suspicious network activity.
- Establish relationships with cyber information-sharing organizations.

- Incorporate appropriate security requirements in all contracts with third party vendors and service providers.
- Provide mandatory privacy and security awareness training on a recurring basis to all personnel.

Responsive Measures

- Mobilize your incident response team to assist with incident mitigation and data recovery.
- Investigate the scope and nature of the incident, compiling information relating to the source of the breach and the type of data compromised.
- Preserve evidence for later forensic examination.
- Reach out to the affected parties as soon as possible to notify them about the breach.

- Consult with legal counsel to determine whether to provide notice to Federal and state regulators.
- Review your cybersecurity liability insurance policy to determine which claims are covered.
- Conduct a post-incident review and incorporate lessons learned into internal policies and procedures.

PRIMARY CONTACTS

Adrienne S. Ehrhardt
Partner • Practice Group Chair, Privacy & Cybersecurity
asehrhardt@michaelbest.com
T. 608.283.0131

Elizabeth A. Rogers
Partner
earogers@michaelbest.com
T. 512.640.3164

Ryan T. Sulkin
Partner
rtsulkin@michaelbest.com
T. 312.596.5836

Rebecca L. Gerard
Associate
rlgerard@michaelbest.com
T. 312.596.5872