Data Breach Toolkit

The volume of data security breaches is only expected to increase in the months and years ahead. For most businesses, it is not a question of if a data breach will occur, but rather when and how often. This Data Breach Toolkit is meant to equip you with a few best practices so that your business is better prepared in the face of a breach.

How to prepare for a data breach

1. Know your data. What personal information does your business collect, store, use and share? Is all of the information that you collect and store necessary for the services you provide? Where is personal data stored and what steps are taken to keep it secure? Does any of this data come from outside the United States? What federal, state or global laws apply to the data you collect? Are there any unique laws that apply based on your business or type of information?
2. Update policies and procedures.
   - Inventory the corporate data privacy and security policies and procedures that are in place, including the date these policies were last updated.
   - Update your website privacy policy and terms of use.
   - Make sure any written policies and procedures are consistent with actual business practices. A disconnect between policy and actual practice can lead to an action by the Federal Trade Commission (FTC) along with a 20-year consent decree and fines.
   - Develop and implement appropriate record and email retention and destruction policies.
3. Train and educate. Educate and train all employees on ways to avoid introducing malware into your system and networks.
4. Vendor management. Scrutinize the privacy and data security practices of your vendors and make sure appropriate obligations and protections are included in your vendor agreements.
5. Insurance. Cybersecurity insurance is available to cover many of the costs you might incur in the event of a data breach. Make sure that coverage is sufficient and includes legal counsel, computer forensics, remediation costs, notification costs, public relation costs and litigation costs, if necessary, to defend against government or private actions.
6. Incident response team and plan. Every business should prepare for a potential data breach by creating and implementing an incident/data breach response plan. Someone should be in charge of managing the team and process. It could be someone in IT or legal with experience handling such events. The plan should include input from upper management, legal, information technology, operations, finance, human resources, communications and marketing. Members of the response team include legal, IT, computer forensics and public relations. The plan should track and record incidents and data breaches as they are discovered. Records should be maintained of any investigation and result.
7. Information security program. All businesses should have adequate safeguards and systems in place to protect personal data in their possession and a process to systematically handle any unauthorized access or data breach. There are a number of security standards and frameworks that can be followed such as those released by the National Institute of Standards and Technology (NIST) of the International Standards Organization (ISO). If you handle or store credit card data, you may be required to comply with the standard known as PCI-DSS. Your privacy

compliance and information security program should be customized to your specific business based on the type of information you collect, store and share.

8. **Encryption.** Most data breach notification laws are not triggered to the extent data is made unreadable via encryption. Businesses should be sure to encrypt any personal data transmitted over unsecured networks.
9. **Limit access.** Use multifactor authentication and limit access to only those who need to access the data for a specific purpose.
10. **Limited data collected.** Only collect and store personal information that you need. The collection and storage of unnecessary personal information is an invitation to potential liability.

What to do following a breach

Follow your incident response plan and mobilize your team as necessary. When you discover unauthorized access or a data breach, the top priority is to stop the access and protect the data. You may need to engage outside legal and computer forensics resources to assess the incident and take any corrective actions. These outside resources should be listed in your incident response plan. This will save valuable time when prompt action is necessary. Make sure any outside forensics team is paired with legal counsel early on to maintain attorney-client privilege of any forensic reports and investigations.

The incident response team will make an initial determination as to whether an unauthorized access or breach occurred that requires notification. Legal counsel will determine based upon the forensics investigation what federal, state and international laws are implicated and if law enforcement should be called.

Notification requirements under all relevant state and federal laws must be reviewed promptly to make sure that if a breach notice is required, it is timely, and complies with any other statutory requirements.

Communicating with customers about a data breach

Reputational harm is often a greater concern than potential government fines or penalties. Include an experienced public relations firm or communications person on your incident response plan.

Notifying other parties about a data breach

Depending on the nature of the data breach you may need to notify regulators, credit reporting agencies, state attorneys general, and the media or law enforcement. The laws vary on when or if notification is required. It is important to engage legal counsel who can advise when notification is required, to whom, and ensure any deadlines are not missed.

In some cases businesses have entered into customer contracts that require notification of any unauthorized access or data breach. If the business has cybersecurity insurance one of the first calls should be to the agent.

For further assistance contact:

Michael Cohen
michael.cohen@gpmlaw.com
(612) 632-3345

In collaboration with the Minnesota Department of Employment and Economic Development Gray Plant Mooty recently published ***A Legal Guide to Privacy and Data Security***, which includes additional information regarding privacy and data security. The Guide is available for download without charge from Gray Plant Mooty's website at http://www.gpmlaw.com/ Practices/Intellectual-Property-Technology-Pri-vacy/Global-Privacy-Cybersecurity-Data-Protection. You can also obtain a paper copy by calling Michael Cohen at (612) 632-3345.