Data Security Incidents and Breaches: Prevention and Response

From Burke, Warren, MacKay & Serritella, P.C.

I. Data Security Incidents and Breaches – Large Corporations Are Not the Only "Targets"

While you have no doubt read about or even been the victim of a data security breach suffered by a large company like Target or Equifax, small, privately-owned businesses are increasingly the targets of data security attacks. In fact, according to Symantec's Internet Security Threat Report, hackers have targeted small businesses at an increasing rate each year. Every privately-owned business, regardless of size, must be prepared to protect its data and operating systems and the data entrusted to it by its employees and customers. It also need to be prepared to comply with the varying data security breach notification requirements of each state, and in certain circumstances federal law, if a breach occurs.

KEY TERMS

Data security incident: a security event where the integrity, confidentiality or availability of data is compromised.

Data security breach: an incident that results in the confirmed disclosure – not merely potential exposure – of data to an unauthorized party.

Personally identifiable information ("PII"): information that can be used on its own or with other information to identify, contact, or locate a person. What constitutes PII varies from state to state for breach notification purposes.

Ransomware attack: a cyber-attack where a business or other entity is locked out of its data unless a ransom is paid, or where the hacker threatens to publish data unless a ransom is paid.

II. Who and How?

According to Verizon's 2017 Data Breach Investigations Report,[1] 75% of breaches are perpetrated by individuals and groups outside the affected organization. Hacking techniques were used in 62% of the breaches according to Verizon's 2017 study, and 81% of hacking-related breaches were accomplished by using either stolen or weak passwords. In 66% of these hacking breaches, malware installed via email attachments or links was used. Other main causes of breaches are physical attacks on data, such as card skimmers, or by unauthorized use or access by current or former employees.

[1] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

III. Prevention First

Given these threats, the first line of defense is assuring your business has strong data security. Keep highly sensitive information, including business secrets, account information, and employee and customer PII, segregated from other data and only allow necessary individuals to access that data. Likewise, systematically monitor your networks, accounts, and devices for suspicious activity. Employ a robust password policy. Although the National Institute of Standards and Technology "NIST," recommends that passwords be at least eight characters long and include at least one number and one non-alphanumerical character, NIST recognizes that adding additional characters to a password boosts its security exponentially. Wherever possible, require dual- or multi-factor authentication for access to the company's most sensitive data. Employee training and awareness regarding email scams, emphasizing not clicking on links from emails masquerading as messages appearing to come from the business or from Microsoft or other email service providers, and also the need for employees to report such emails quickly, are best practices. Finally, think ahead by setting up an incident response plan detailing who in your organization is responsible for doing what in the event of an incident or breach.

In addition to maintaining strong data security, consider whether cyber insurance makes sense for your business. Cyber insurance can insure against losses in the event of a data breach, can provide coverage for legal fees and costs associated with data breach notifications, and may cover costs for a forensic analysis of how the attack occurred and what data was affected.

IV. Incident Response – So You've Been Breached

Even with best practices in place, incidents and breaches can still happen, and you must act fast to locate the source of the breach, secure your data, and notify the affected parties. The basic steps to take in the event of an incident or breach are:

- ***Implement your incident response plan***
  - Notify the appropriate internal response team of the nature of the breach
  - Assess what happened with your internal or external IT specialist

- ***Secure data immediately***
  - Contact your internal or external IT specialist to assist
  - Change passwords

- ***If necessary, contact law enforcement***
  - If a hacker is actively in your system, or in the event of ransomware attack, notify local authorities or the FBI immediately

- ***Contact your insurance carrier and attorney***
  - Once your data is secure and, if necessary, you have contacted law enforcement, contact your insurance carrier to determine what cyber-coverage you have and

contact your attorney to develop an action plan for complying with the applicable data breach notification requirements

V. Data Security Notifications

After a data security breach, you must notify the affected individuals, typically in writing and within a certain timeframe, that their data has been compromised. Even small businesses must do this, and in most instances even where only one person's data may have been affected. Businesses can be subject to fines or civil liability for failure to comply with data breach notification requirements.

A. Federal Law Requirements

Currently, there is no overarching federal data security breach notification law. Instead, different federal laws cover different entities and types of information. For example, the Gramm Leach Bliley Act covers financial institutions such as banks and lending institutions. The Fair Credit Reporting Act covers creditors who access credit reports, and the Health Insurance Portability and Accountability Act ("HIPAA") covers health plans, health care providers, health care clearinghouses and their "business associates" (i.e. companies that perform services for such entities and receive "protected health information" from such entities. If your business is covered by these laws, your data security and notification requirements are more stringent.

B. State Law Requirements

Each state has its own data breach notification statute, which defines what is considered PII, who must be notified (individuals, state attorneys general, and/or credit reporting agencies), and what specific information must be contained in each notification. The state of residence of the person whose data was breached determines which state law applies. That means even if you are an Illinois business, if your customer or employee who resides in California's data was breached, you must comply with California law.

- ***Is Notification Required?*** Some states only require notifications if the business determines there is a risk of harm to individuals. In other states, mere unauthorized access to data requires notification. As a business, you may determine that notification is the best course of action to protect your reputation, and avoid legal risk, even where you are not positive data was stolen.

- ***What is Considered PII?*** In most states Social Security numbers, driver's license numbers, and account numbers are PII. Some states require additional steps if healthcare information, PINs, or passwords are breached.

- ***How Fast?*** The time for notification varies from thirty days to "as soon as reasonably possible." Some states will give extra time if there is an ongoing law enforcement investigation. In Illinois the standard is the most "expedient time possible and without unreasonable delay."

- ***Whom to Notify?*** Some states, like Connecticut and New York, require that the state Attorney General be notified in the event of any breach. Other states like California only require notification if over a certain number of residents are affected. Illinois does not require notification to the Attorney General unless the entity breached is a state agency.

- ***What to Say?*** The content of the notice varies greatly by state, but most require a brief explanation of what data was affected and information on how to contact the "big three" credit bureaus (Equifax, Experian and TransUnion). Some states require the notice to identify the number of residents affected. Illinois law explicitly states that the number of Illinois residents affected should ***not*** be included in the notification.

- ***How to Notify:*** Sending "actual" written notice via U.S. Mail is the legal standard for most states. This means if the letter bounces back, you need to find the person's correct address and re-send the letter. In some instances, you may be able to provide notice via email, posting, or the media, but only if mailing written notice will cost over a certain amount (identified in each statute) or is otherwise impossible.

- ***What to Offer?*** A small number of states require businesses to offer credit monitoring or protection in the event of a breach. Illinois does not require businesses to offer credit monitoring.

VI. Conclusion

Maintaining strong data security practices and emphasizing employee awareness of cyber threats is an essential part of doing business today even for small businesses. Aside from the liability risk, protecting your data is integral to protecting your reputation and your brand. Still, even with excellent data security measures in place, breaches happen. Having a plan in place is critical for responding quickly to secure your company's data and to make the appropriate notifications to affected individuals.

For further information, please contact Susan Overbey, soverbey@burkelaw.com, 312-840-7051. Susan is a partner at Burke, Warren, MacKay & Serritella, P.C., serves as the firm's Security and Privacy Officer, Co-Chair of the Consumer Financial Services Litigation Group and Chair of the firm's Technology Committee and has assisted companies in responding to data security breaches large and small.