Shumaker

DECEMBER 18, 2018 | PUBLICATION

Client Alert: Mitigating the Consequences of a Data Breach – The Steps You Can Take Right Now

SERVICE LINE

Data Breach Response Team

RELATED PROFESSIONALS

Douglas A. Cherry

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

News reports about data breach and cybersecurity incidents have increasingly become commonplace. While much of the news coverage has focused on data breach or hacking incidents impacting large institutions – Facebook, Equifax, Uber, Home Depot, Target, yahoo, the U.S. Office of Personnel Management – an alarming number of small businesses have also suffered cyberattacks. Any notion that cyber criminals are only interested in large institutions or that a data breach is unlikely to affect your organization, is emphatically false. The truth is, your business has likely already suffered a cybersecurity or data breach incident and will so again in the future.

Data breach and cybersecurity incidents demand your attention. According to a 2017 Ponemon Institute/IBM study of 419 major data breaches from around the globe, the average cost to respond to a data breach was $3.62 million per breach. Out of all the data breaches studied, those within the United States were the most expensive at an average cost of $7.35 million per breach. In addition to financial considerations, data breaches can also negatively impact an organization's reputation and goodwill. In recent months privacy concerns have taken center stage as consumers demand greater protections and accountability at the highest level. Is your organization prepared?

This article is a primer on the steps an organization can take today to mitigate against the consequences of a data breach when it occurs. The takeaway from this article is simple:

- The occurrence of a data breach is not a question of *if*, but *when*.
- Steps should be undertaken now to mitigate the potential risk and consequences of a data breach.
- Protecting and maintaining the security of data is an ongoing responsibility.If a data breach were to occur, it can't be swept under the rug. Statutory authority has dramatically increased and there can be severe consequences for failure to report to those affected.

1. What is a data breach?

A data breach is generally defined as an event where personal information (frequently referred to as PII), such as an individual's name, in combination with another piece of information (e.g. social security number, financial account number, or other sensitive information) is viewed, copied, or otherwise accessed by someone that does not have permission to access such information. The occurrence of a data breach typically triggers legal duties under state, federal and in some cases, international law.

A data breach often occurs through such means as hacking, malware, ransomware, payment card fraud, unintended disclosure, lost or stolen electronic device or insider access.

Currently, all 50 states and the U.S. territories of the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have statutory laws that include specific procedures for data breach incidents. The European Union General Data Protection Regulation ("GDPR"), which is effective May 25, 2018, also contains requirements for reporting a data breach to supervisory authorities located in the EU. Depending upon the circumstances of a particular breach, a duty may be imposed upon the person or organization that suffers a data breach to report the occurrence to law enforcement, credit reporting agencies, and the people whose information was accessed during the data breach, and in some instances, to provide assistance, such as credit monitoring services.

2. Steps you can take before an attack occurs (NOW!)

Maintaining good organizational cybersecurity requires being proactive. The following are a few preventative measures that your organization can take to help mitigate the risks of a data breach.

- Develop an actionable, Written Information Security Program ("WISP"), which should include an Incident Response Plan ("IRP").The WISP is part of a comprehensive strategy for managing information security throughout the organization.The plan needs to be tailored to your specific organization and needs.
    - An IRP is a detailed plan that is part of the WISP and is aimed at the immediate response to a data breach or cyber security incident.The IRP should identify members of an incident response team, and clearly define each team member's roles and responsibilities.The incident response team typically consists of members from the organization's information technology team, risk management, outside counsel, a computer forensics consultant or firm, public relations, and other organizational decision makers.
    - Outside counsel and the forensic consultant with experience in responding to data breach matters should be identified in the IRP before any cybersecurity or data breach incident to ensure there is no delay in bringing either of them on-board in response to an incident.
    - Additional Elements of the IRP often include (i) procedures for notification to the organization's insurer (often a prerequisite for insurance coverage); (ii) instructions from counsel regarding handling privileged communications and protected work product; (iii) criteria and procedures for communicating information to senior management or the board; (iv) contact information for a public relations expert to preserve the organization's goodwill and to assure potentially affected customers, employees and affiliates that the organization is addressing the problem aggressively

with steps to protect them from harm;(v) a contact for credit monitoring services or other identity theft mitigation services; (vi) a list of contracts containing obligations of the organization in the event of a data breach.
    - Once the IRP is in place, be sure to practice the plan prior to the attack (i.e. have a "fire drill").Simply developing the plan is not enough.The whole incident response team should be involved in and feel comfortable with their roles under the IRP.
- Since you cannot protect the information you do not know exists, a data inventory is often a great starting point for an organization developing a WISP.A data inventory is a snapshot of how data is used throughout an organization at a particular point in time.
- Make sure the plan also addresses your dealings with vendors/affiliates that share or store your data.
- Consider acquiring cyber insurance for your organization.Evaluate and obtain a policy that is tailored to your organization's particular risk.Find an insurance agent experienced in this field.Once you acquire coverage, take time to carefully review the policy to be sure you understand its requirements, and any prerequisites that may be required for coverage of certain incidents.For example, your cyber insurance policy may require you to have a policy for employees concerning how personal information must be transmitted to customers as a prerequisite to providing coverage for an employee inadvertently disclosing personal information to a third party.
- Make sure your organization has appropriate technology, services, and controls in place before an attack occurs. Consider:
    - imposing access controls to data;
    - requiring secure passwords and authentication as prerequisite for access to personal information;
    - storing sensitive personal information securely and using technologies to protect such information during transmission;
    - securing and monitoring (through logs) remote access to the organization's network;
    - put procedures in place to ensure you routinely re-visit and maintain best practices in data and network security, and have a plan to address vulnerabilities that may arise; and
    - secure physical paper, media, and devices (encrypt laptops), lock file cabinets, etc.

When you suspect or learn that a data breach has occurred, the first step will be to implement your IRP, which will detail procedures for contacting experienced outside counsel, a forensic consultant, notifying your insurer, address public relations concerns, notifying law enforcement, and providing notifications or alerts.

As a final comment, consider what information to keep. The more PII a business maintains, the more liability may exist. Since server space is so inexpensive, it is not uncommon for archived PII to be hacked. Consider keeping such data on "off the grid" servers. Also, attempt to pass responsibility for maintaining necessary data to reputable outside vendors whose job is to implement state-of-the-art security standards. When doing so, pay careful attention to service provider agreements. Such agreements should contain data security contract clauses that require vendors to have a plan that meets certain standards and to carry cyber-insurance.

3. Conclusion

By implementing a WISP, IRP, and routinely practicing for a data breach incident, your organization will be better prepared to respond to a cyber-attack or data breach incident. In the aftermath of a data breach or cyber-attack, time is of the essence. Having a plan that you can quickly call into action can have a significant impact in limiting the effects of such incidents.