THE NATIONAL CYBERSECURITY SOCIETY

DATA BREACH NOTIFICATION

DID YOU KNOW?

- ✓ Data breaches continue to increase each year, outpacing the previous year.
- ✓ One way to minimize the impact of a data breach is to completely remove the data once it is no longer needed - from all sources including your backup.
- ✓ Know what data you have and keep an inventory of it and where it is stored.
- ✓ There are 48 different data breach notification laws in the U.S.

WHAT IS A DATA BREACH & WHO SHOULD I NOTIFY?

A data breach is an incident whereby an unauthorized individual has accessed confidential or sensitive data. The data could be personally identifiable information (PII), personal health information (PHI), financial data, trade secrets or intellectual property. The data could be viewed or stolen (or held for ransom). When the data is used by a criminal to create a new identity – that is identity theft.

A data breach could also include an incident in which an individual simply views data they do not have authorization for regardless of theft. Additionally, malicious intent does not have to be a factor for a data breach to have occurred. A data breach could be due to a systemic flaw, or accidental exposure of the data by an authorized individual.

Currently there are 48 different state data breach notifications in the U.S. If you believe your company has been the victim of a data breach, obtain **legal** advice. PII is defined differently in each state, so it's important to have a professional guide you through the process. Given that the results of a data breach can be so devastating to a user, most states have specific laws governing data breaches.

HOW DO I KNOW IF I'VE BEEN BREACHED?

There are several ways to know if you've been a victim of a data breach. For instance, you may have been contacted by a credit card company or by law enforcement.

WHAT SHOULD I DO?

- **Stay calm** to prevent further damage and take control of the situation. Think of each step before you take it.
- **Start taking notes.** You can use this how to guide to assist you through the steps needed and the documentation insurance or investigators may want to know.

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Data Breach Notification continued…

- **Call your lawyer and take notes.** Your attorney will advise you of your responsibilities under local, state and federal law.
- **Notify important parties.** Communicate with employees, business partners, customers, vendors, and credit bureaus based upon your crisis communication action plan. It is important to communicate based upon the audience, your strategy and the data to be reported at the time. It may take weeks to months to completely understand what has occurred, so what you report when will change. Plan now with a crisis action plan, see our how to guide on crisis management.
- **Call your insurance company** to see if you are covered and to see if there are any requirements under your coverage. If you do not have cyber insurance, affordable plans are available for small businesses. As a minimum, your cyber insurance policy should cover remediation, data notification to affected parties, annual identity monitoring for victims and legal fees.
- **Contact police and take notes.** Notify local law enforcement of the incident and document your contact to fulfill your legal obligations.
- **Change passwords.** Change the passwords on your point-of-sale systems, cash registers, and any business systems.
- **Be prepared for an investigation.** You may be required to hire a 3rd party investigator or forensic expert by your credit card company or another business partner.

Ongoing –

- **Document everything.** Document all aspects of the data breach, including records, logs, and steps undertaken. Be prepared to describe the locations of customer data and other PII stored within your business. This is very important for the insurers, law enforcement, and other investigators. Plan now to respond to a data breach and develop a Data Inventory Log that defines all places where sensitive data is stored.
- **Review your lessons learned.**

Regardless of how the data breach occurs, the consequences are very much the same. It is the responsibility of the organization collecting the information to ensure the data is secure. This is particularly relevant when the information collected is Personally Identifiable Information (PII).

It is important to note that many times data breach laws do not only apply to organizations physically located in the state. They can be applicable to an organization if they do business in the state, or collect user information from individuals in the given state. This is particularly relevant in if the organization does business online, as their customer base could be from a multitude of states.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.