Protecting Against Data Breaches

Five steps you can take right now.

BY JULIE EISENHAUER

WE'VE ALL READ the news about data breaches. Each new incident makes it clear that businesses large and small need to address security and assurance.

KEY STATISTICS*

- An estimated **78%** of all companies and organizations in the United States suffered some sort of data loss or theft within the last two years.
- **44%** of small businesses say they have been a victim of cybercrime at least once.
- **More than half** of U.S. small businesses have experienced at least one data breach.
- **75%** of respondents in a survey say they've had or expect to have a data breach resulting in negative publicity.

FIVE PRACTICAL STEPS

Security experts say data breaches are unavoidable. It's not a question of if companies will become victims of a data breach, but when. However, there are five practical steps a business can take to help protect against data breaches and mitigate the potential harm in the event of a breach.

1. Perform an inventory. It is critical to inventory the locations that store personally identifiable information (PII). PII is defined as information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. Personal information includes such things as first and last name, social security number, biometric records, date and place of birth, mother's maiden name, address, email address, driver's license number and financial account information. Determine which PII information your business requires, what data are collected, how these data are secured, and who has access to the data and under what circumstances. Once you have identified the location of your data, move it to more appropriate locations as needed.

2. Encrypt computers. It is a best practice to encrypt all laptops and publicly accessible desktop computers. Encryption encodes messages or information on a computer in a way that only authorized individuals can read. It doesn't prevent intrusion, but it does make the data unreadable and unusable by an intruder. Encryption software is affordable and highly effective in protecting data. Consider using a data encryption method that is Federal Information Processing Standard (FIPS) certified, which means it complies with federal government security protocols. Frequently monitor your systems to ensure that the encryption is still active.

3. Implement an intrusion detection system. An intrusion detection system includes a device or software application that monitors network or system activities for malicious activity. Detecting an intrusion early allows for a quicker response, reducing the cost per data record stolen. In order to determine what is considered malicious or "unusual" activity, the business should first define what is considered "normal" activity.

4. Develop a detailed plan for quicker response. Every business should plan for the unexpected and that includes the loss or theft of data from your business. Companies that implement a data breach response plan have the tools to act quickly, reducing the harm caused by a data security breach. The plan should document the names of the response team members, including outside vendors such as the attorney, forensic accounting and/or IT security firm and insurance broker. The plan should also document the steps to access the scope of the breach and secure the premises, identify compromised data and eradicate hacker tools, and establish guidelines for notification.

5. Train your staff. Businesses train their staff for daily, on-the-job duties. If you haven't already done so, expand staff training to include the appropriate use of your computer systems, assessing and transferring data, safe web browsing rules, and how to identify threats such as phishing. Encourage your employees to use passwords that are random, complex, changed regularly and that are closely guarded and not written down. Ensure all staff are trained on recognizing suspicious activity and that they are familiar with the company's data security plan.

A data breach can have great consequences that include not only the direct costs of attorneys and forensic experts, but also the indirect costs resulting in the loss of customers and damage to your brand. Take action now to secure your important data and mitigate the potential harm in the event of a breach.

**Data derived from the* Verizon 2014 Data Breach Investigation Report *and the* Ponemon Institute 2013 Report.

JULIE EISENHAUER, CPA, is an audit and assurance shareholder at Clark Nuber PS, specializing in privately held companies. Reach her at jeisenhauer@clarknuber.com and follow her on Twitter @EisenhauerJulie.