10 Tips to help prevent a data breach

THE HARTFORD

Small businesses are increasingly at risk for data theft, also known as data breach. According to the Verizon 2013 Data Breach Investigations Report (DBIR), organizations with fewer than 100 employees comprised 31% of data breach incidents investigated in 2012.[1] You can minimize your business's risk of data breach by taking these essential steps.

Data breach defined

Loss, theft, accidental release or accidental publication of Personally Identifiable Information (PII) including:

- Social Security number
- Bank account number
- Credit or debit card numbers
- Driver's license number
- Patient history and medications

What's a strong password?

- Is at least 8 characters long
- Does not contain your user name, real name, or company name
- Does not contain a complete word
- Is significantly different from previous passwords
- Contains a combination of upper- and lowercase letters, numbers and symbols

1. Secure sensitive customer, employee or patient data.

- Store paper files and removable storage devices (such as thumb drives and CDs) containing sensitive information in a locked drawer, cabinet, safe or other secure container when not in use.
- Restrict access to sensitive data to those who have a need to know. Give employees access to only the information they need to do their jobs – whether it's online or in paper form.

2. Properly dispose of sensitive data.

Shred documents containing sensitive data prior to recycling. Remove all data from computers and electronic storage devices before disposing of them.

3. Use password protection.

Password protect your business computers – including laptops and smartphones – and access to your network and accounts. Require employees to have a unique user name and a strong password that is changed at least quarterly.

4. Control physical access to your business computers.

Create user accounts for each employee to prevent unauthorized use of your business computers. Laptops can be easy targets; make sure they're locked in place when unattended. Also limit network access on computer stations located in public spaces, such as the reception area.

continued

5. Encrypt data.

Encryption helps protect the security and privacy of files as they are transmitted or while on the computer. Install encryption on all laptops, mobile devices, flash drives and backup tapes, and encrypt emails that contain sensitive information.

6. Secure access to your network.

- A firewall prevents outsiders from accessing data on your network. Enable your operating system's firewall or purchase reputable firewall software. Be careful with free firewall software as it may actually contain "scareware" that can infect your network.
- Allow remote access to your network only through a secure manner such as a properly configured Virtual Private Network (VPN).
- If you have a Wi-Fi network for your workplace, make sure it's secure, encrypted and hidden so that its network name or "Service Set Identifier" (SSID) can't be picked up by the public. Also be sure a password is required for access.

7. Protect against viruses and malicious code ("malware").

Install and use antivirus and antispyware software on all of your business computers. Don't open email attachments or other downloads unless you're sure they're from a trusted source.

8. Keep your software and operating systems up to date.

Install updates to security, Web browser, operating system and antivirus software as soon as they become available. They contain "patches" that address security vulnerabilities within the software and are your first line of defense against online threats.

9. Verify the security controls of third parties that have access to your data.

Before working with third parties that have access to your data or computer systems or manage your security functions, be sure their data protection practices meet your minimum requirements and that you have the right to audit them. Not only do you want to ensure that your customer and business data is secure, but if a breach occurs on their watch, you could still be held liable and may be required to take all the necessary steps toward recovery – including notifying customers, monitoring credit, paying penalties or fines, etc.

10. Train your employees on your company's security principles.

Last but not least, make sure your employees understand your data protection practices and their importance. Document your policies and practices and distribute them to your team. Review your practices regularly and update them as required. Be sure to retrain your staff as updates are made.

[1] Percentage is an approximation based on the Verizon 2013 Data Breach Investigations Report.