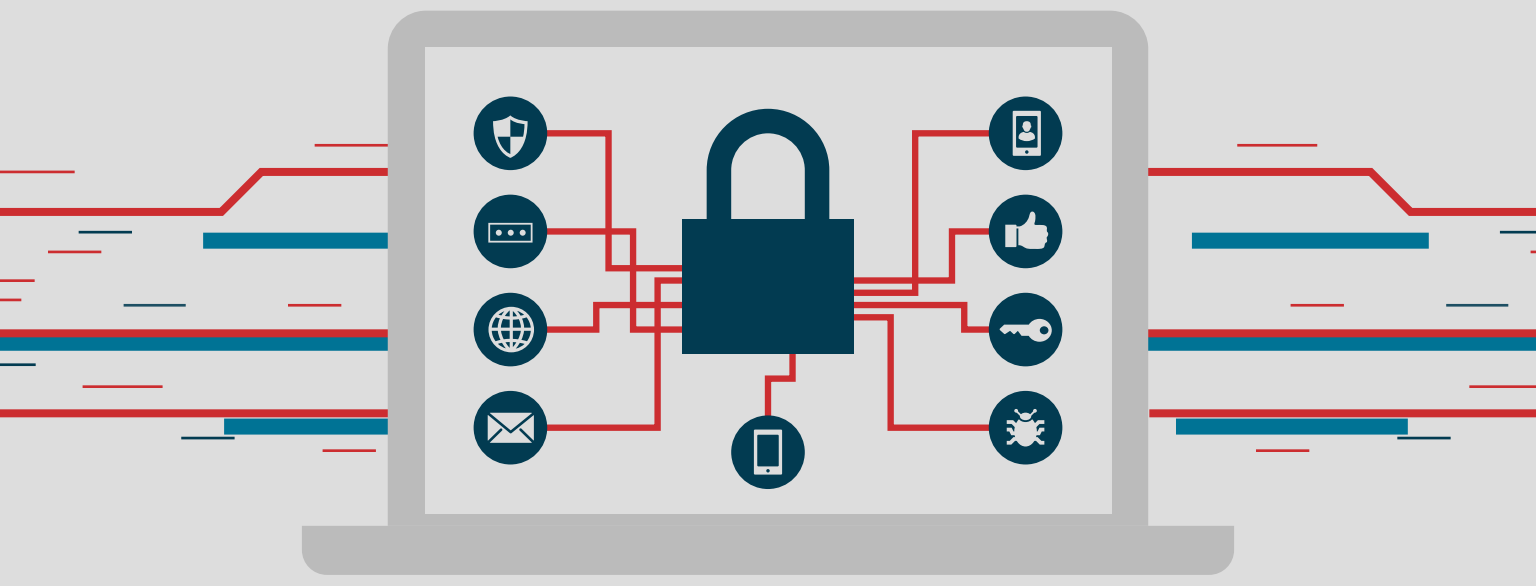

9 KEY ELEMENTS OF A DATA SECURITY POLICY

1 **Safeguard data privacy.** Employee and customer data should be kept confidential and secure.

2 **Establish password management.** Your policy should cover all employees plus temporary workers. Passwords should never be shared, and password complexity standards should be established.

3 **Govern Internet usage.** Balance your need for employee productivity with restrictions based on your security concerns.

4 **Manage email usage.** Email is a favorite way for hackers to steal information. Set clear standards for message content, encryption and file retention.

5 **Govern and manage company-owned mobile devices.** Implement a formal process. At a minimum, require employees to protect their devices from theft and establish password protection.

6 **Establish an approval process for employee-owned mobile devices.** Employees who have access to company information via their personal devices accept the limitations and controls imposed by the company.

7 **Govern social media.** Active governance can help make sure employees speak within company guidelines and follow data privacy best practices.

8 **Oversee software copyright and licensing.** Adhere to the terms of software usage agreements and employees should be made aware of any usage restrictions.

9 **Report security incidents.** All employees and contractors should know the procedure for reporting incidents of malware and what steps to take to help respond.

Share this infographic with your coworkers and associates to help them **#HarnessRisk**.

Visit **travelers.com/resources/cyber-security** for more cyber security tips for your business.

TRAVELERS