

Triple-I Offers Businesses Seven Ways to Guard Against Data Breaches

October 22, 2020

SHARE THIS



DOWNLOAD TO PDF

For immediate release

New York Press Office: (917) 923-8245; media@iii.org

NEW YORK, Oct. 22, 2020 – Data breaches can be either averted or mitigated if businesses take the proper precautions to safeguard their financial and reputational risks, according to the [Insurance Information Institute](#) (Triple-I).

In a [brief video](#), the Triple-I outlines seven ways businesses can protect themselves from data breaches given the growing number of cyberattacks.

- 1. Understand your [cyber risks](#).** Businesses are vulnerable to cyberattacks through hacking, phishing, malware, and other methods.
- 2. Train Staff.** Those engaged in cyberattacks find a point of entry into a business' systems and network. A business' exposure can be reduced by having and enforcing a computer password policy for its employees.
- 3. Keep Software Updated.** Businesses should routinely check and upgrade the major software they use.
- 4. Create back-up files and store off-site.** A business' files should be backed up either as an external hard drive or on a separate cloud account. Taking these steps are vital to data

recovery and the prevention of ransomware. Ransomware is when a cyberattack results in a situation where a business is asked to pay a fee to regain access to its own data.

- 5. Ensure systems have appropriate firewall and antivirus technology.** A business should evaluate the security settings on its software, browser and email programs.
- 6. Establish a Data Breach Plan.** A business should remind its employees to review periodically the data breach detection tools installed onto their computers. If a data breach occurs, employees must notify the business immediately to prevent further loss.
- 7. Protect your business with insurance coverage designed to address cyber risks.** Cyber insurance coverage typically provides protection for costs associated with data breaches and ransomware.

When businesses are in the market for a cyber insurance policy, or looking to renew an existing one, these risks should be considered, the Triple-I states:

- **Liability**—A business may be liable for costs incurred by its customers and other third parties as a result of a cyberattack or other Information Technology (IT)-related incident.
- **System recovery**—A business would need the financial resources either to repair or replace its computer systems or lost data.
- **Customer Notification**—In several states, businesses which store customer data must notify customers if a data breach has occurred or even if one is just suspected to have happened.
- **Regulatory fines**—If a data breach results from a business' failure to meet federal or state compliance requirements, the business may incur substantial monetary fines.
- **Class action lawsuits**—Large-scale data breaches have led to class action lawsuits filed on behalf of customers whose data and privacy were compromised.

The Triple-I has a full library of educational videos on its [YouTube Channel](#). Information about Triple-I mobile apps can be found [here](#).

Back to top

