Munich RE

10 ways to help prevent a data breach

Lessons from ethical hackers

Risk Solutions

The Boiler Inspection and Insurance Company of Canada

390 Bay Street
Suite 2000
Toronto, ON, M5H 2Y2
Tel: (416) 363-5491
munichre.com/HSBBII

Connect with us

What's the best way to protect a business from a data breach? "Think like a hacker," say the experts, and improve security so cybercriminals will move on to the next target.

HSB Group's security specialists teamed up with a group of 'white hat' (ethical) hackers to develop a list of risk management tips that can help your business protect the private information that you keep on customers, employees and others.

1. **Outsource payment processing.** Avoid handling card data on your own. Reputable vendors, whether for Point-of-Sale or web payments, have dedicated security staff that can protect that data better than you can.

2. **Separate social media from financial activity.** Use a dedicated device for online banking. Use a different device for email and social media. Otherwise, just visiting one infected social site could compromise your banking machine and your savings account.

3. **Think beyond passwords.** Never reuse them and don't trust any website to store them securely. You can never tell when a website has already been hacked and your password has been exposed. Set up a two-factor authentication: this sends a secret code to your phone verifying your identity.

4. **Educate and train employees.** Establish a written policy about data security, and communicate it to all employees. Educate employees about what types of information are sensitive or confidential and what their responsibilities are to protect that data. Also, most scams and malicious attacks arrive through email so be sure your team is prepared and alerts others when they are received.

1866

HSB BI&I

5. **Stay informed.** Evaluate the entire chain of events in a potential attack. From assessing your email infrastructure to your users' responsiveness to your browser's vulnerability, identify where your organization is most at risk. Then question the security posture of your business lines, vendors, suppliers or partners.

6. **Stop transmission of data that is not encrypted.** Mandate encryption of all data. This includes data 'at rest' and 'in motion'. Also consider encrypting email within your company if personal information is transmitted. Avoid using Wi-Fi networks: they may permit interception of data.

7. **Secure your browser.** With the growing popularity of watering holes – malicious code installed on trusted websites – how do you know which websites you can trust? Forget individual patches. Focus on keeping up to date with the latest version of your browser. Then, test your browser's configuration for weakness.

8. **Secure your operating system.** It's far easier to break into older operating systems like Windows XP or OSX10.6. Take advantage of major security improvements baked into newer operating systems.

9. **Secure your router.** It connects your computer to the internet. Make sure someone can't intercept all the data sent through it. It's important to set a strong admin password on your router and a WPA2 password on your Wi-Fi.

10. **Secure your data.** Whether you lose data to an accident or an attack, you'll always be glad to have a backup. Ideally, your backups should be encrypted and off-site in case there's a fire or burglary.

NOT IF, BUT HOW